MILLENNIUM MEDIA

Network Security Analysis Report

Author Name: Shahrokh Tahmooreszadeh
Version 1.0
Date: 30/11/2022

Approval

Name	**Jae Summers**	**Title**	**Network Manager**
Signature	Digitally Signed	**Date**	30/11/2022

Table of Contents

Author Name: Click here to enter your name. 1
Version 1.0 1
Date: Click to enter the date. 1
1. Current security threats and vulnerabilities 4
2. Implementation of Perimeter security 5
2.1 Firewall rule 5
A. Router, firewall settings 5
B. Evidence of implementation 6
C. Testing of firewall rule 7
D. Purpose and benefit of the implementation to prevent identified threats and vulnerabilities 7
2.2 Server and network hardening 7
A. Server and network settings 8
B. Evidence of implementation 8
C. Purpose and benefit of the implementation to prevent identified threats and vulnerabilities 9
2.3 Authentication and user account controls 10
A. Authentication and user account control settings 10
B. Evidence of implementation 11
C. Test results and outcomes of the above implementation 11
D. Purpose and benefit of the above implementation to prevent identified threats and vulnerabilities 16
2.4 Encryption 16
A. Encryption settings 16
B. Evidence of implementation 17
C. Test results and outcomes of the above implementation 19
D. Purpose and benefit of the above implementation to prevent identified threats and vulnerabilities 19
3. Design and conduct function and performance tests 20
3.1 OpenDNS implementation 20
3.2 Router setting configuration 21
3.3 Conducting function and performance tests 22
3.4 Conducting system audit 25
3.5 System asset details report 31
3.6 Network traffic performance report 31
4. Design and implement security system 33

4.1 Network scan results 33
4.2 System audit results 33
4.3 Antivirus and anti-malware solution 35
4.4 Data backup and sync solution to protect from environmental threats 36
5. Analysis of test results and recommendations 46
5.1 Network security risks identified during the testing process 46

1. Current security threats and vulnerabilities

Asset Categories	Threats and Vulnerabilities	Priority
Network	Considering clients typically correspond through email (sometimes including attached files), phishing attacks (attachments) are probable. Considering there is no firewall set up on the network, there is a risk of attacks from hackers.	2
Software	Some desktops have not been updated with latest viruses' definitions and have not performed a system scan for a considerable amount of time. Solution: they should all be managed centrally and updated with latest viruses' definitions regularly. Firefox browser is a free and open-source software which has got some vulnerabilities. Solution: It should always be updated to make sure we are protected against these vulnerabilities.	1
Hardware	Having only one server in the whole network is a single point of failure. Solution: we can set up multiple servers for high-availability configurations. In such configurations, multiple servers either operate at the same time to provide more capacity or operate in sequence to provide failover protection. Considering all organisation's staff have access to the server room can directly put the data at risk of being destroyed or stolen. Solution: Only authorised staff should have access to the server room and it should be monitored by security cameras.	4
System	Servers and other network equipment are configured with the same administrator username and password. Solution: using different administrator username and password. All computer systems are accessed using domain user accounts having a password policy that allows a length of six characters or numbers. Solution: the minimum password length should be at	3

	least 8 characters (a mix of uppercase, lowercase, symbos and numbers)	

2. Implementation of Perimeter security

2.1 Firewall rule

A. Router, firewall settings

How to set up Access Control for website blocking on TP-Link Wireless Router

Step 1: Log in to your router's web management page.

Step 2: Go to **Access Control > Host**, then click **Add New**...

Select '**IP Address**', then enter a short description for the host rule you want to define in the '**Host Description**' box. Enter the IP address range on your network that you want to block access to.

Click **Save** - the new Host rule will now show up on the "**Host Settings**" page

Step 3: Go to **Access Control ->Target**, then click **Add New...**

Step 4: Select **Domain Name** as the mode type. Create a unique description (e.g. target_1) for the target in the Target Description field and enter the domain name, either the full name or the keywords (for example TP-LINK) in the Domain Name field.

Step 5: Go to **Access Control > Schedule** and configure the schedule settings. Click '**Add New**'.

Step 6: Create a unique description (e.g. schedule_1) for the schedule in the **Schedule Description** field and set the day(s) and time period, and click **Save**.

Step 7: Go to **Access Control ->Rule**. On the page displayed, tick "**Enable Internet Access Control**", then select **Allow the packets specified by any enabled access control policy to pass through the Router** as the default filter, then click **Save**.

Click **Add New**, then enter a brief description of the rule in the "**Rule Name**:" box

In the "**Host:**" box, select the Host rule you defined in Step 2

In the "**Target:**" box, select the target rule you defined in Step 3

In the "**Schedule:**" box, select "**Anytime**" (this will make the rule always active)

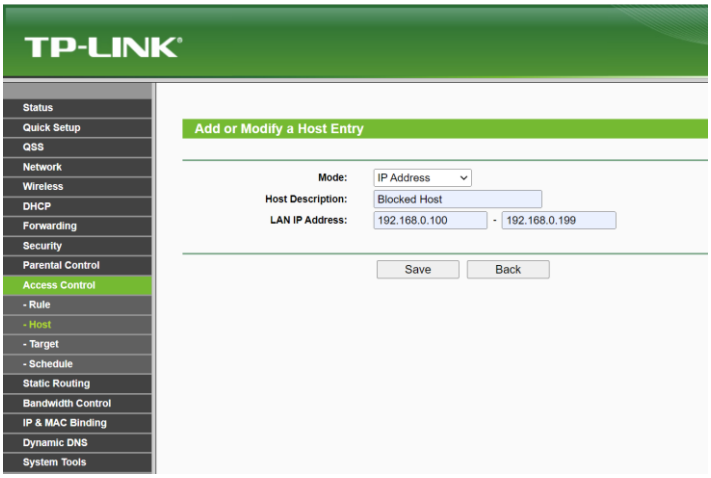
In the "**Action:**" box, select "**Deny**"

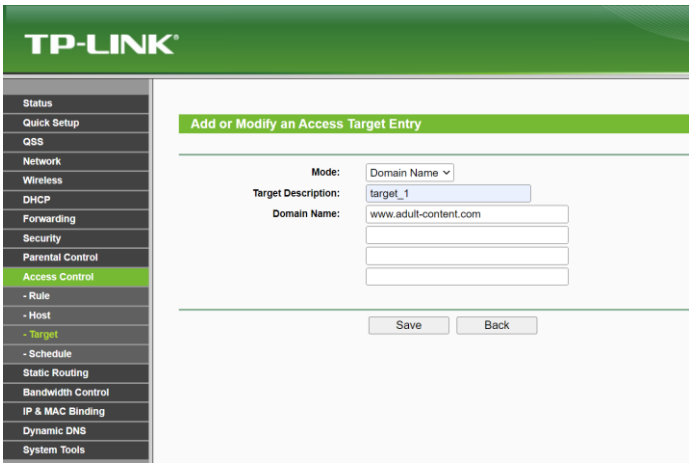
In the "**Status:**" box, select "**Enabled**"

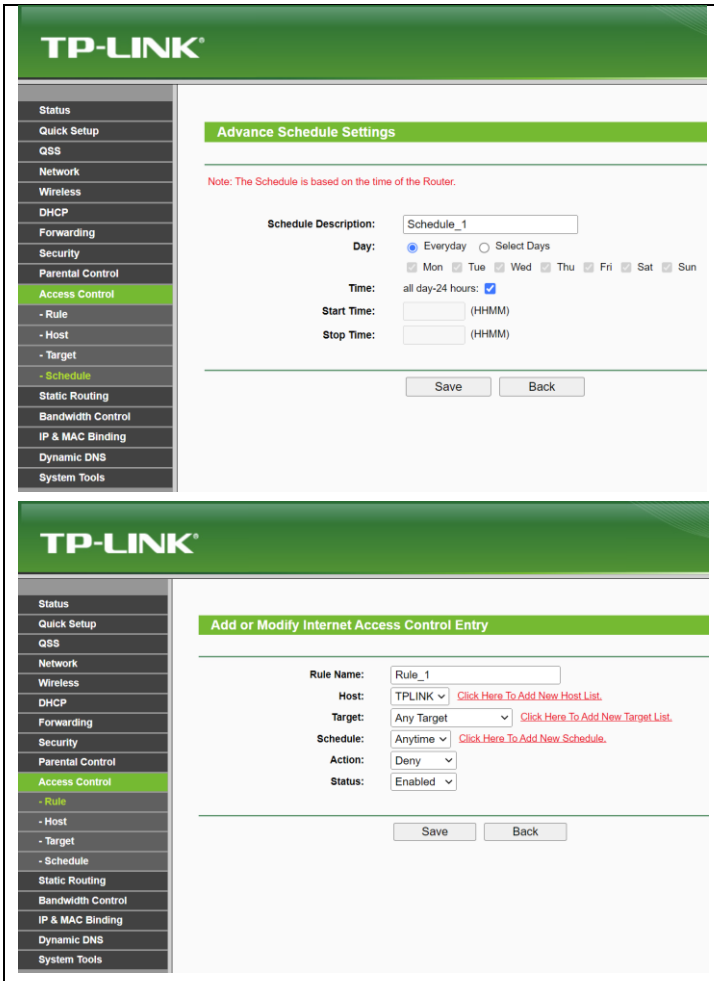
Click **Save** - the new Access Control rule will now show up on the "**Access Control Rule Management**" page.

Now specified host(s) can only visit the target(s) within the scheduled time period.

B. Evidence of implementation







C. Testing of firewall rule

As I used a router emulator, I couldn't take a screenshot of the blocked website.

D. Purpose and benefit of the implementation to prevent identified threats and vulnerabilities

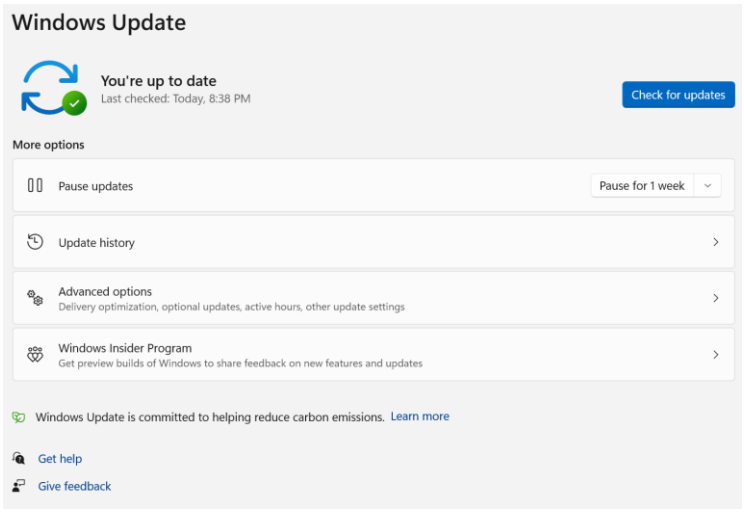
There are many scenarios in which the implementation of a web blocker can have benefits for businesses and organizations. The primary benefit of solutions for blocking web access is that they can prevent Internet users visiting websites harbouring malware or ransomware, websites that are known to be fake and used for phishing attacks, and websites that hide their true identity behind a proxy server.

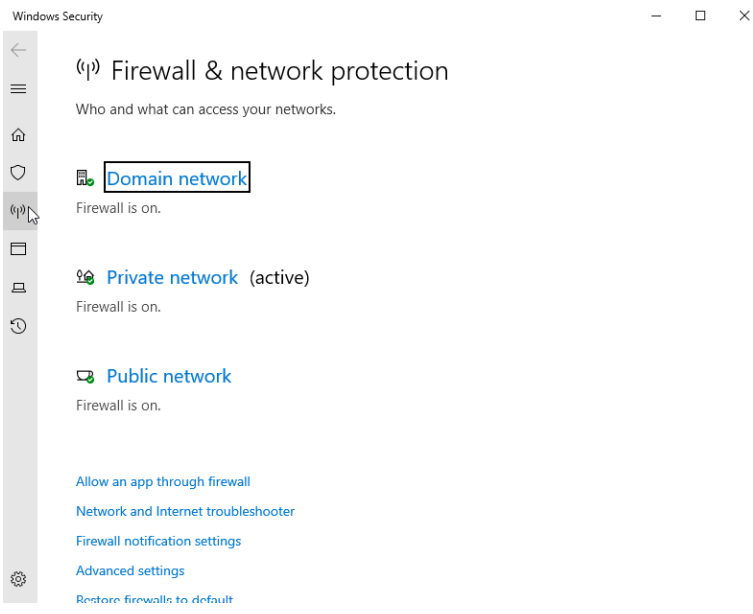
2.2 Server and network hardening

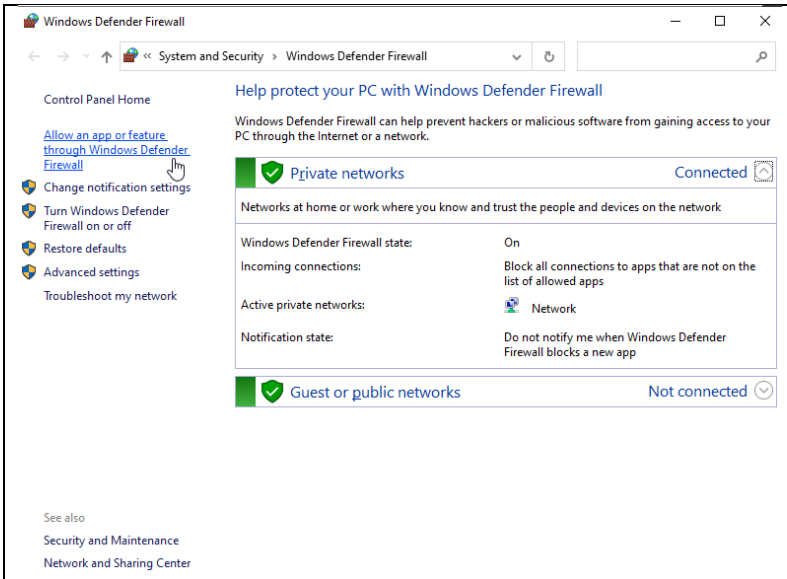
A. Server and network settings

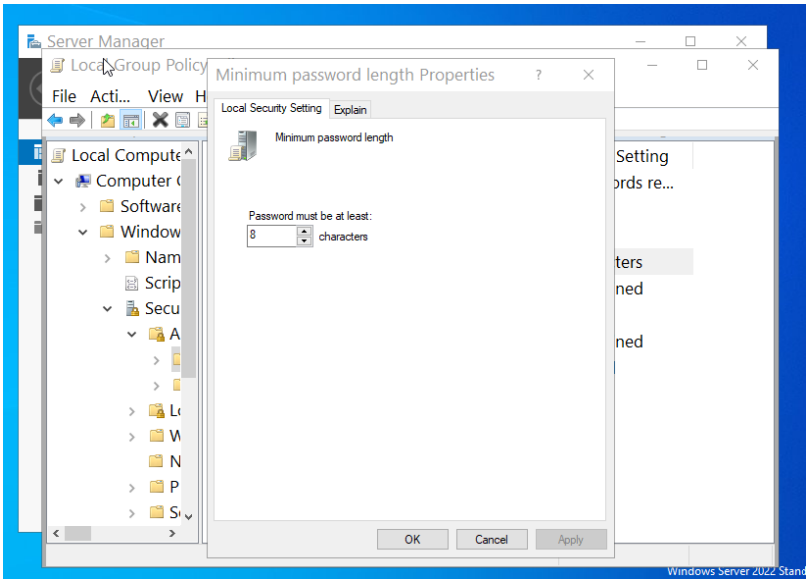
Windows Update: We should make sure that Windows server is up to date.
Windows Firewall: We should make sure that Windows Defender firewall is on.
Minimum Password Length: We should set minimum password length to at least a value of 8.

B. Evidence of implementation









C. Purpose and benefit of the implementation to prevent identified threats and vulnerabilities

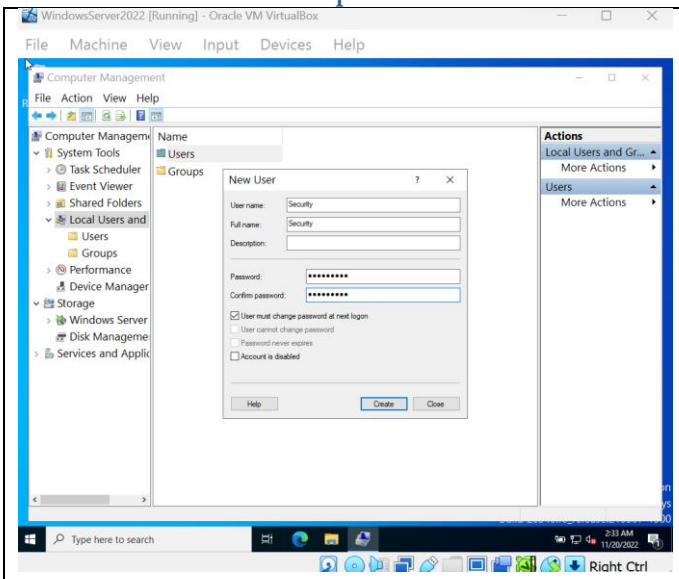
Keeping the servers' operating systems up to date is probably the most important step we can take to secure them since new vulnerabilities are identified and disclosed on an almost daily basis.
Windows defender firewall can help prevent hackers or malicious software from gaining access to the PC through internet or a network.
According to Microsoft recommendation, in most environments, an eight-character password is recommended because it's long enough to provide adequate security and still short enough for users to easily remember.

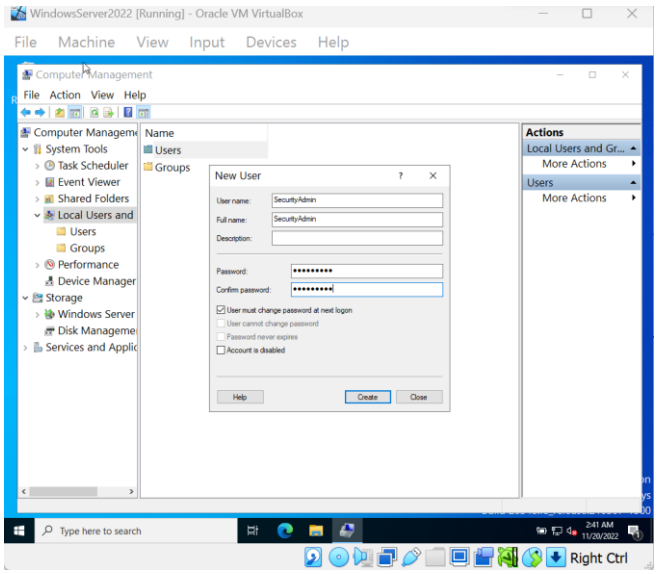
2.3 Authentication and user account controls

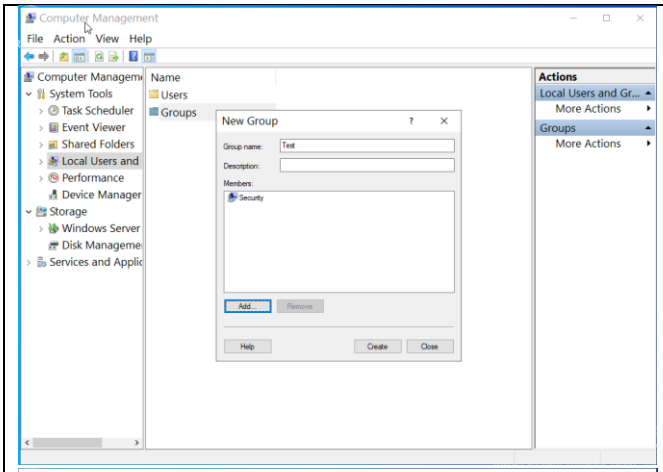
A. Authentication and user account control settings

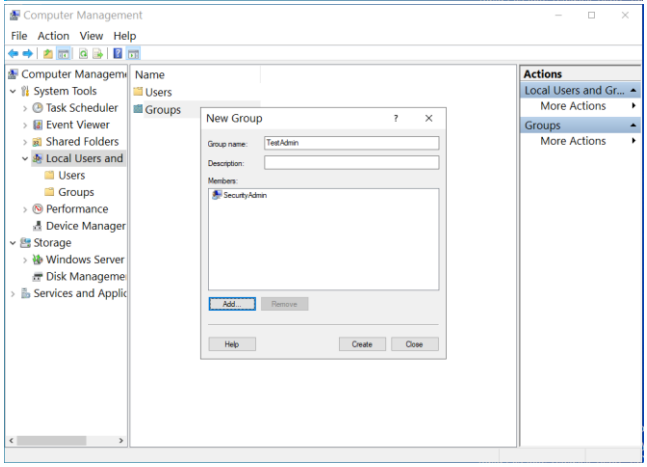
Open Computer Management Click Local Users and Groups Right click the Users folder, and select New User Fill in the list and click Create Right click the Groups folder and select New Groups Fill in the list and add members to the group
Create a new folder in C drive Right click the new folder and select Properties Click Sharing Tab and share this folder Click Security Tab and Click Advanced Click ‘Disable inheritance’ and select the option to ‘Remove all inherited permissions from this object’ Click Add and then ‘Select a principal’ and then look for desired users or groups and add them Change the Permission for the added users or groups and click OK (Select the option to ‘Show advanced permissions’ to see all options available for permissions)

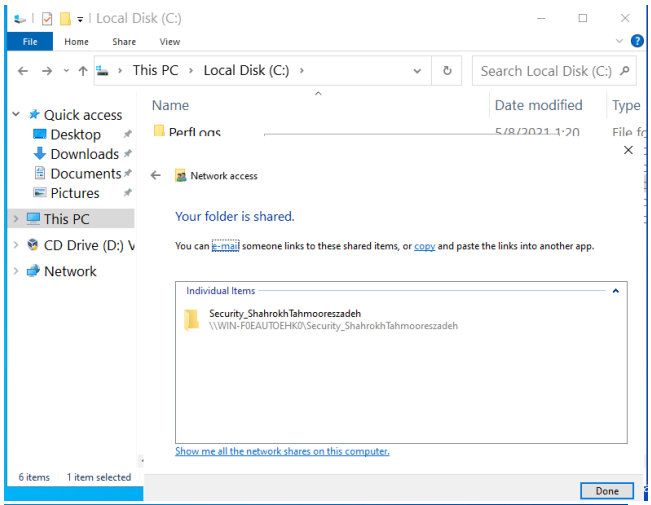
A. Evidence of implementation

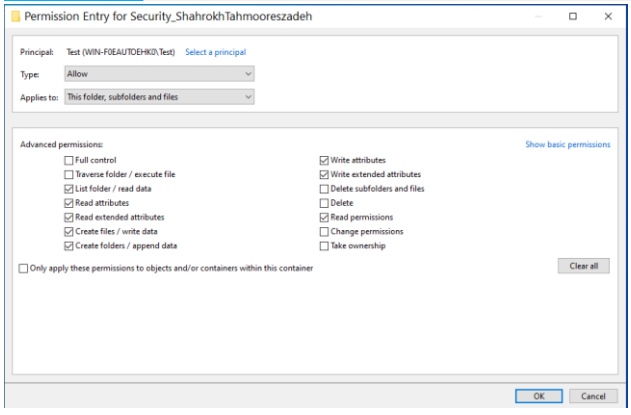


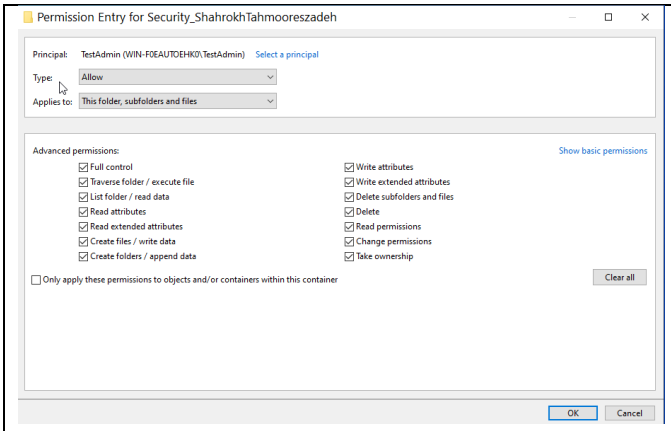



Computer Management
File Action View Help
Computer Management
System Tools
Task Scheduler
Event Viewer
Shared Folders
Local Users and
Performance
Device Manager
Storage
Windows Server
Disk Manageme
Services and Applic
Name
Users
Groups
New Group
Group name: Test
Description:
Members:
Security
Add...
Remove
Help
Create
Close
Actions
Local Users and Gr...
More Actions
Groups
More Actions


Computer Management
File Action View Help
Computer Management
System Tools
Task Scheduler
Event Viewer
Shared Folders
Local Users and
Users
Groups
Performance
Device Manager
Storage
Windows Server
Disk Manageme
Services and Applic
Name
Users
Groups
New Group
Group name: TestAdmin
Description:
Members:
SecurityAdmin
Add...
Remove
Help
Create
Close
Actions
Local Users and Gr...
More Actions
Groups
More Actions

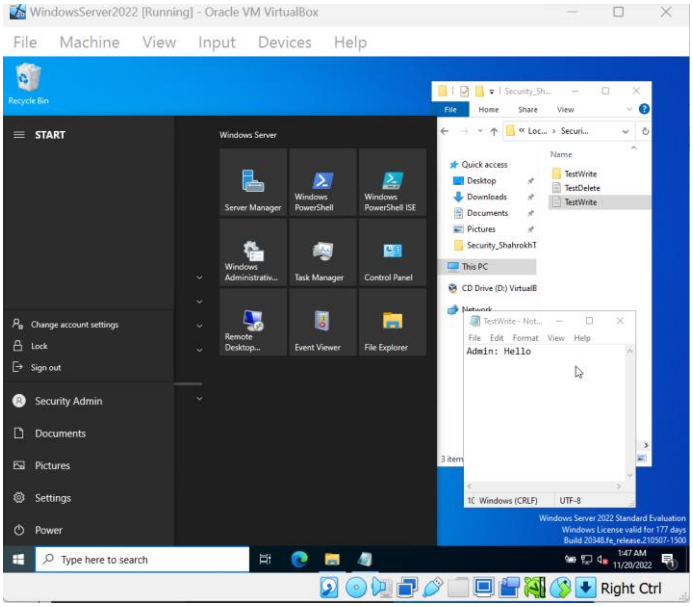

Local Disk (C:)
File Home Share View
This PC › Local Disk (C:) ›
Search Local Disk (C:)
Quick access
Desktop
Downloads
Documents
Pictures
This PC
CD Drive (D:) V
Network
Name
Date modified
Type
Perfl ogs
Network access
Your folder is shared.
You can e-mail someone links to these shared items, or copy and paste the links into another app.
Individual Items
Security_ShahrokhTahmooreszadeh
\\WIN-F0EAUTOEHK0\Security_ShahrokhTahmooreszadeh
Show me all the network shares on this computer.
6 items
1 item selected
Done


Permission Entry for Security_ShahrokhTahmooreszadeh
Principal: Test (WIN-F0EAUTOEHK0\Test) Select a principal
Type: Allow
Applies to: This folder, subfolders and files
Advanced permissions:
Show basic permissions
Full control
Traverse folder / execute file
List folder / read data
Read attributes
Read extended attributes
Create files / write data
Create folders / append data
Write attributes
Write extended attributes
Delete subfolders and files
Delete
Read permissions
Change permissions
Take ownership
Only apply these permissions to objects and/or containers within this container
Clear all
OK
Cancel

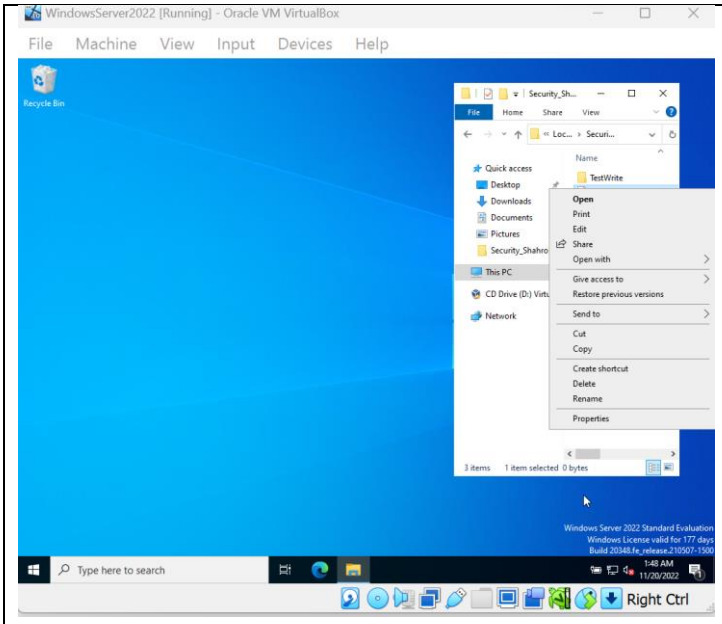


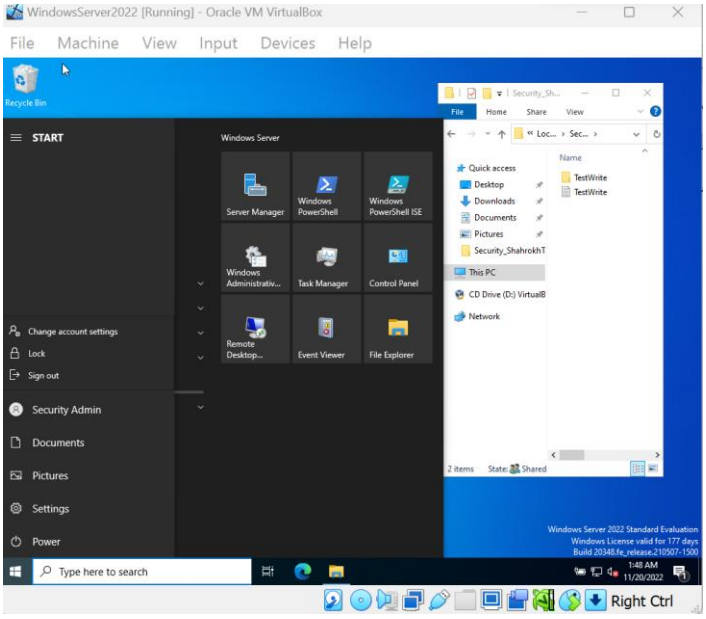
B. Test results and outcomes of the above implementation

Screenshot/s showing that the SecurityAdmin user can Read / Write to the Security_YourName directory

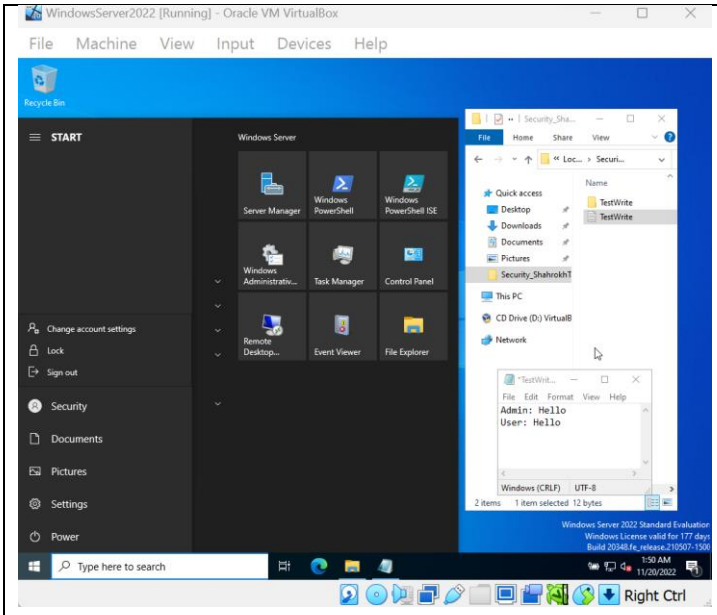


Screenshot/s showing that the SecurityAdmin user can Delete from the Security_YourName directory

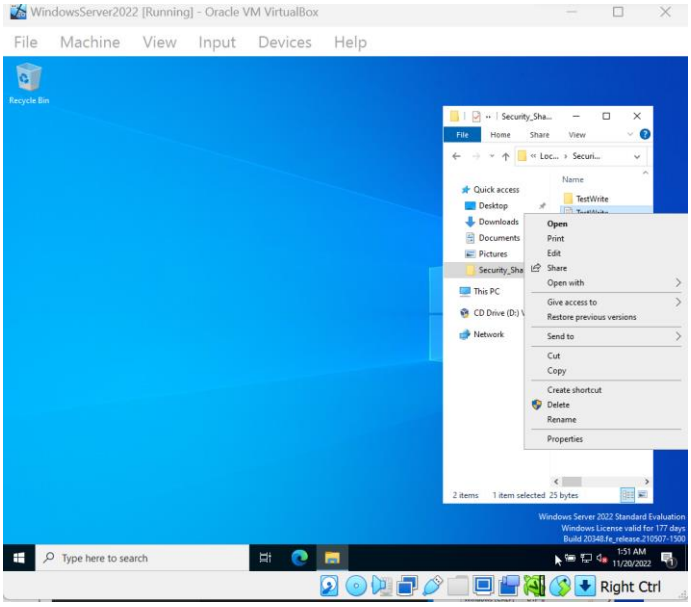


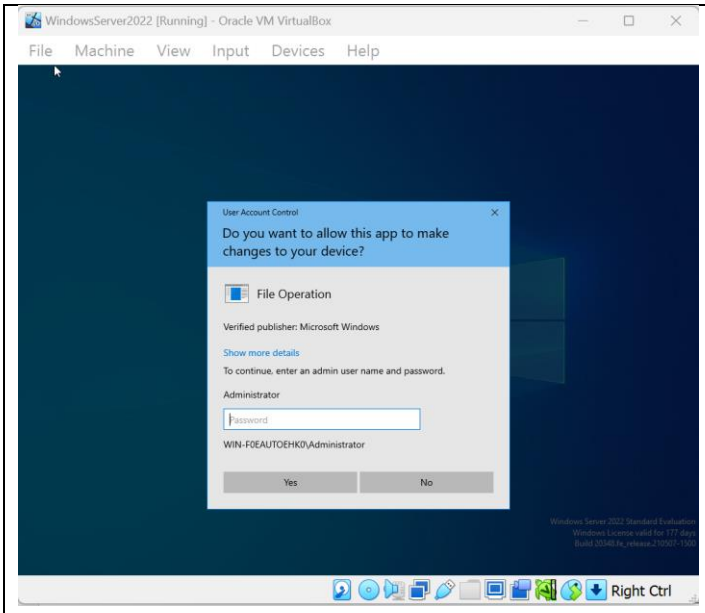


Screenshot/s showing that the **Security** user can Read / Write to the **Security_***YourName* directory



Screenshot/s showing that the **Security** user cannot Delete from the **Security_***YourName* directory





C. Purpose and benefit of the above implementation to prevent identified threats and vulnerabilities

Users' access to resources must be limited and properly controlled to ensure that excessive privileges do not provide the opportunity to cause damage to a company and its resources. Least privilege is the concept and practice of restricting access rights for users, accounts, and computing processes to only those resources absolutely required to perform legitimate functions.

2.4 Encryption

A. Encryption settings

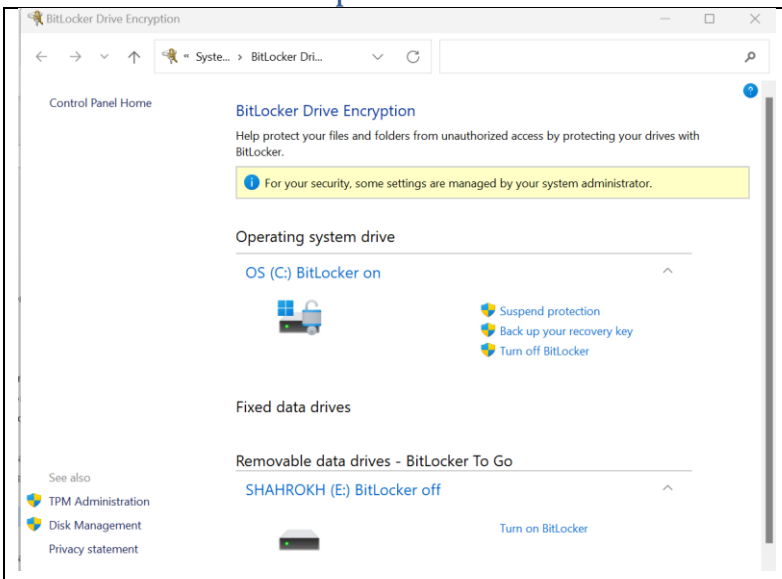
Open Manage Bitlocker in Control Panel

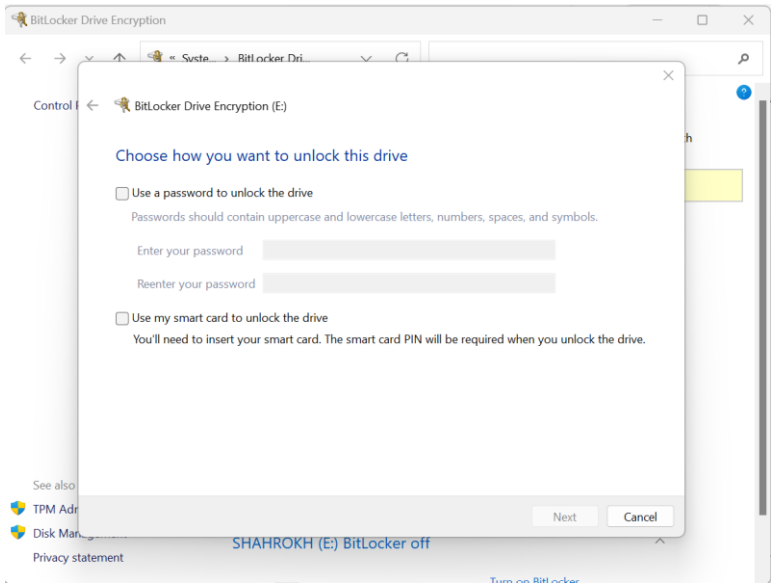
Click Turn on Bitlocker on the selected drive

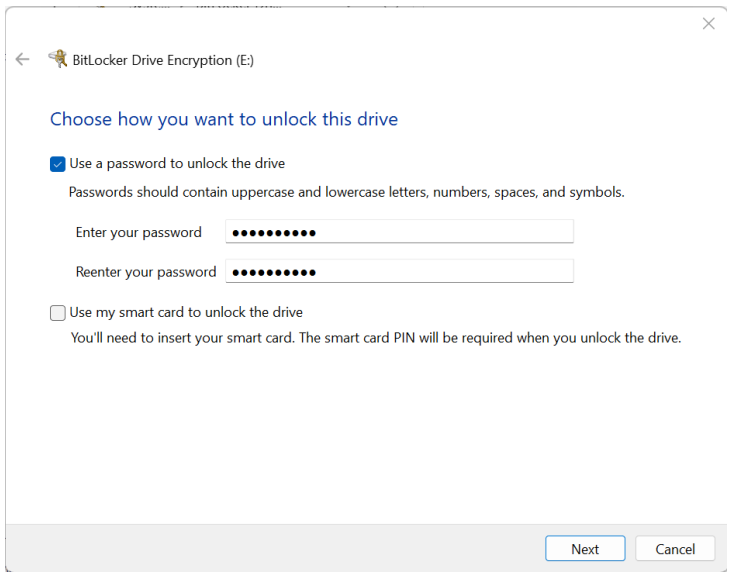
Choose how you want to unlock the drive

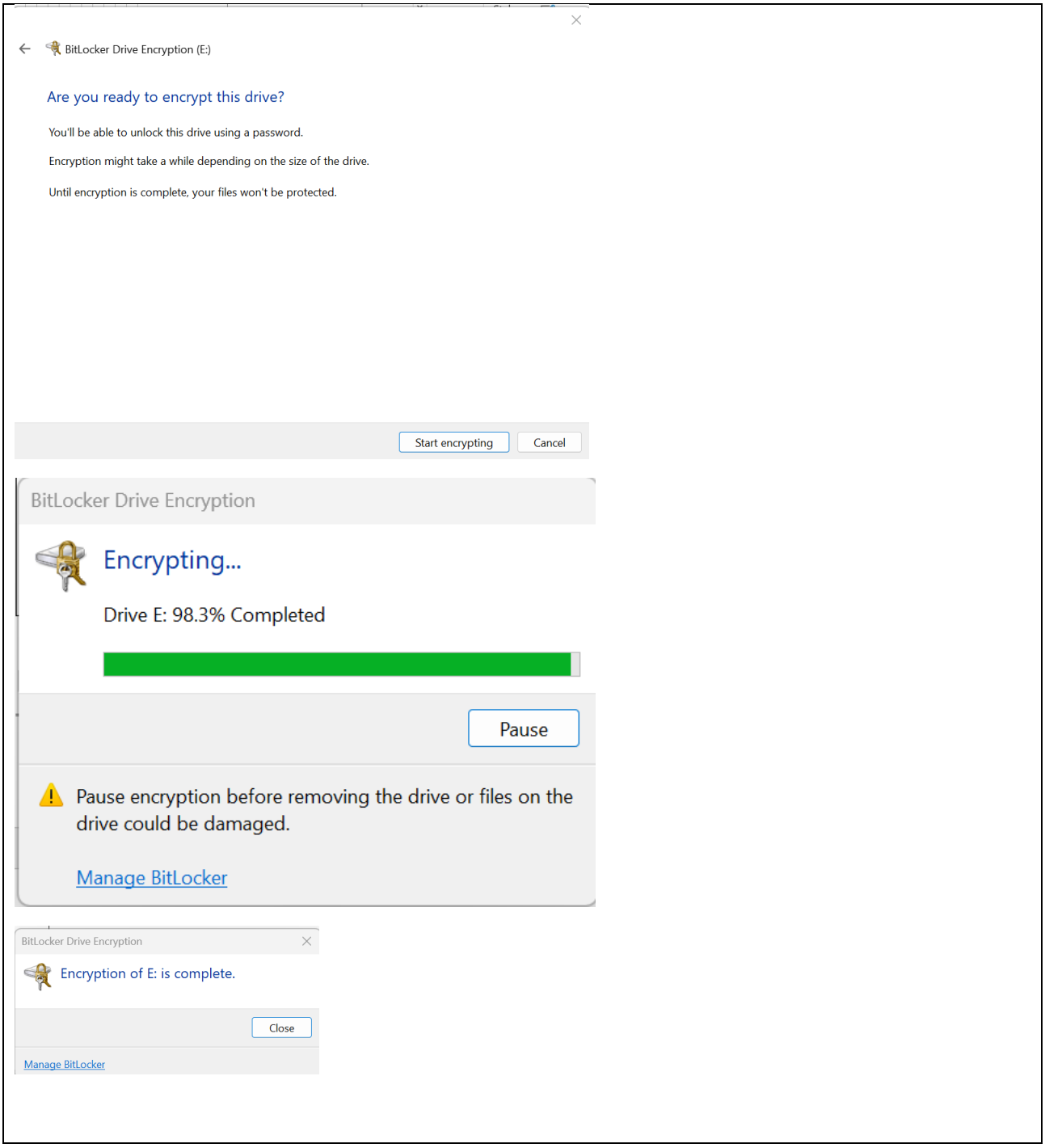
Click Start encrypting

B. Evidence of implementation

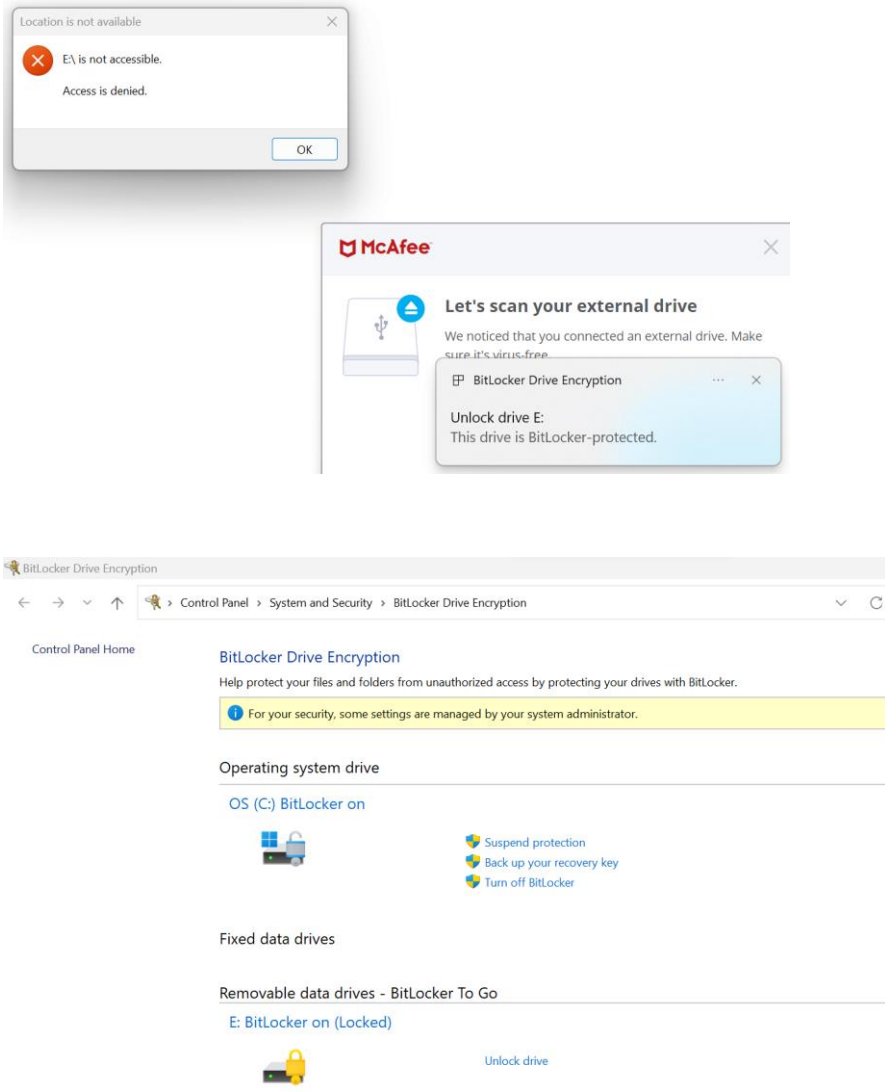







BitLocker Drive Encryption (E:)
Are you ready to encrypt this drive?
You'll be able to unlock this drive using a password.
Encryption might take a while depending on the size of the drive.
Until encryption is complete, your files won't be protected.
Start encrypting
Cancel
BitLocker Drive Encryption
Encrypting...
Drive E: 98.3% Completed
Pause
Pause encryption before removing the drive or files on the drive could be damaged.
Manage BitLocker
BitLocker Drive Encryption
Encryption of E: is complete.
Close
Manage BitLocker

C. Test results and outcomes of the above implementation



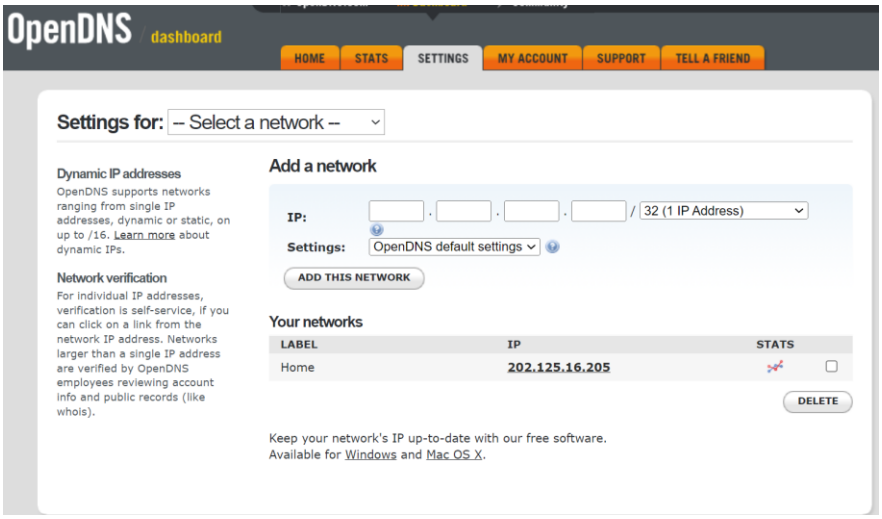
D. Purpose and benefit of the above implementation to prevent identified threats and vulnerabilities

Software solutions to ensuring data security usually involve encryption of some kind, either on a disk or while being transmitted over the network. Encryption is a privacy safeguard and increases the Integrity of our data.

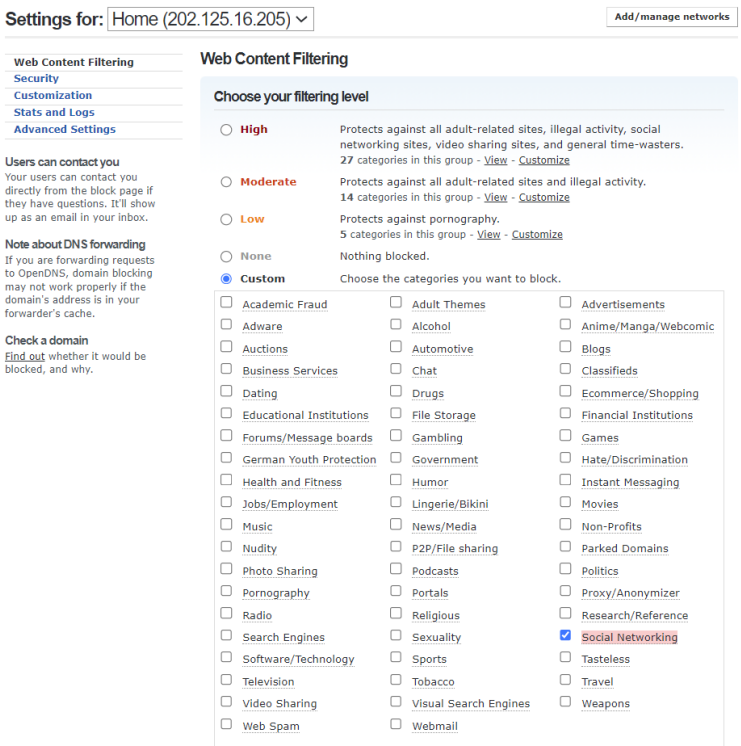
3. Design and conduct function and performance tests

3.1 OpenDNS implementation

Part a:

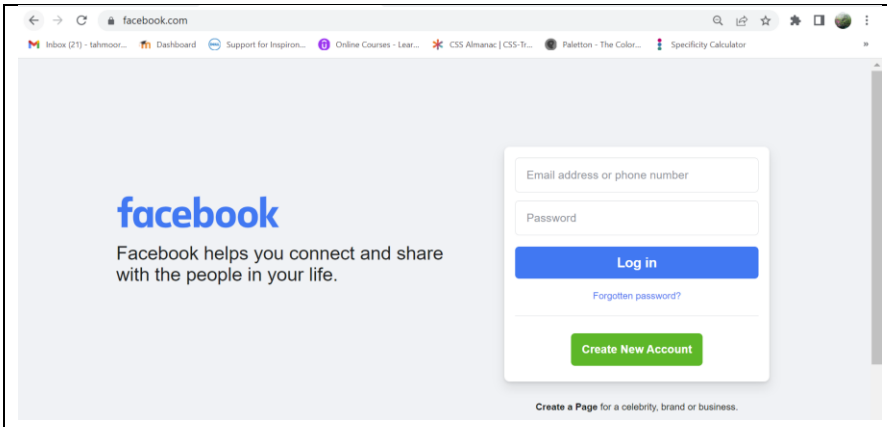


Part b:

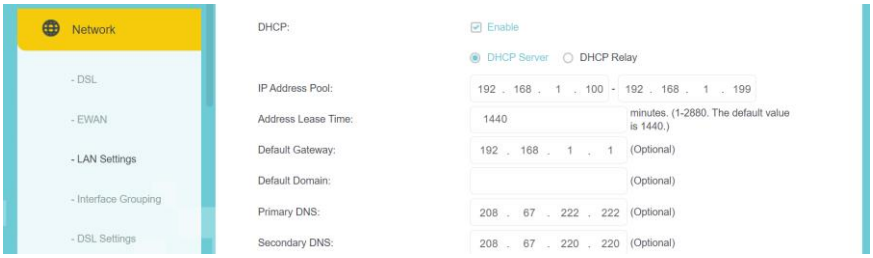


Part c.

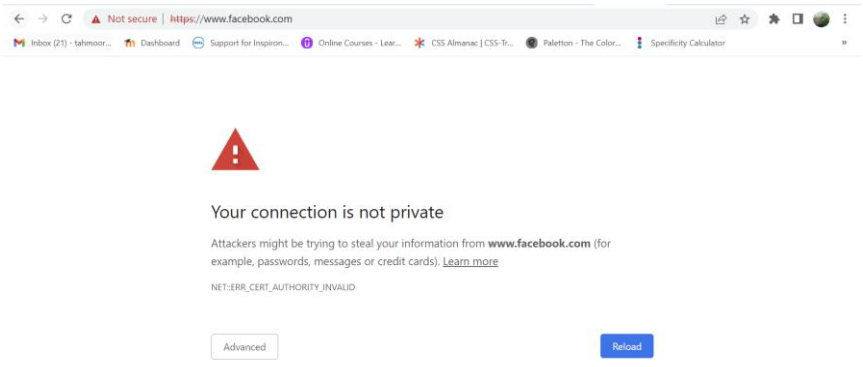
It didn't work!



I added the OpenDNS nameservers to the router:



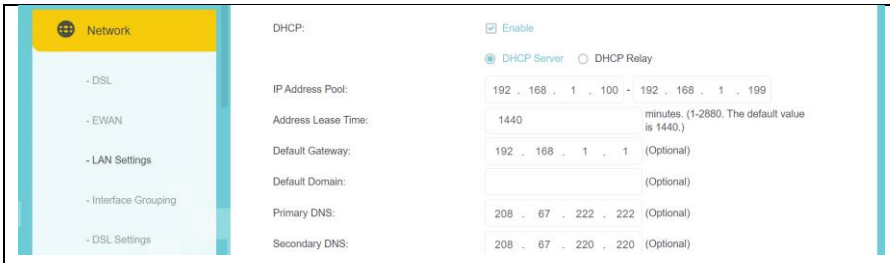
It worked!



3.2 Router setting configuration

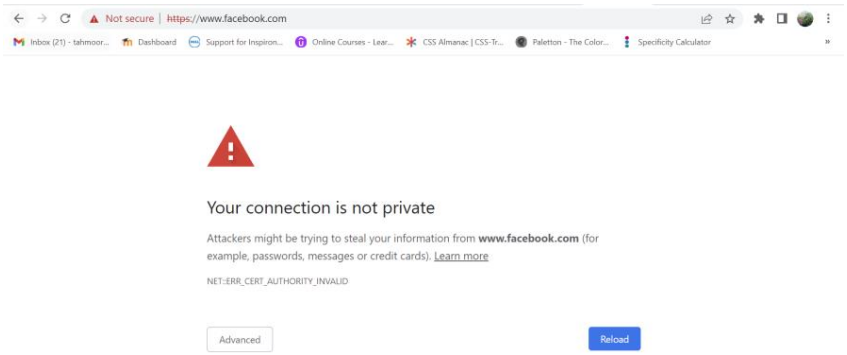
Setting DNS Server on TP Link VR1600v

1. Open the browser and in the **Address Bar** type http://192.168.1.1 and press **Enter** and then **login**
2. On the upper right side of the screen click the Advanced tab.
3. On the lower left side of the screen click on **Network** to expand the menu, then click on **LAN Settings**.
4. Put the DNS server addresses as Primary DNS and secondary DNS
5. Click **Save** to apply the changes.



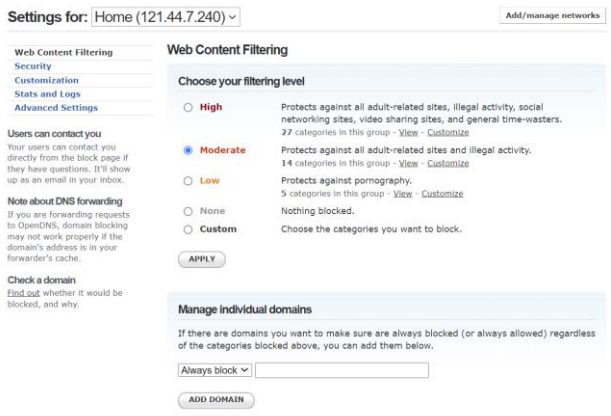

```
IPv4 Address. . . . . . . . . . . : 192.168.1.107(Preferred)
Subnet Mask . . . . . . . . . . . : 255.255.255.0
Lease Obtained. . . . . . . . . . : Wednesday, 23 November 2022 7:38:04 PM
Lease Expires . . . . . . . . . . : Thursday, 24 November 2022 7:38:04 PM
Default Gateway . . . . . . . . . : 192.168.1.1
DHCP Server . . . . . . . . . . . : 192.168.1.1
DHCPv6 IAID . . . . . . . . . . . : 144726352
DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-2A-E7-F7-87-A0-59-50-15-18-05
DNS Servers . . . . . . . . . . . : 208.67.222.222
                                    208.67.220.220
```

6. Check to see whether www.facebook.com has been blocked or not



3.3 Conducting function and performance tests

I set the web content filtering level to moderate including dating websites.

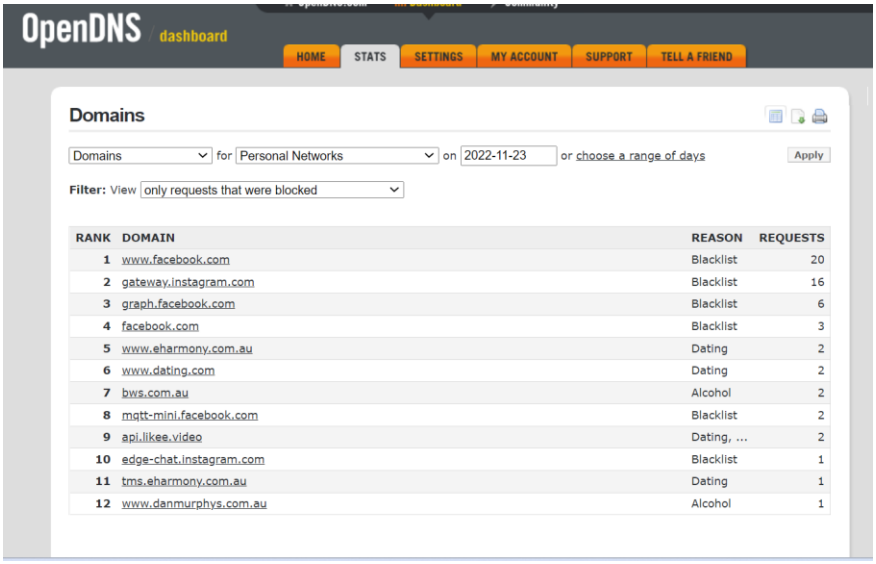


Part a. Metrics: blocked domains on November 23rd 2022

Part b. To measure how well OpenDNS works regarding protecting against all adult-related sites and illegal activity.

Part c. It blocked some of the dating and alcohol related websites but not all of them.

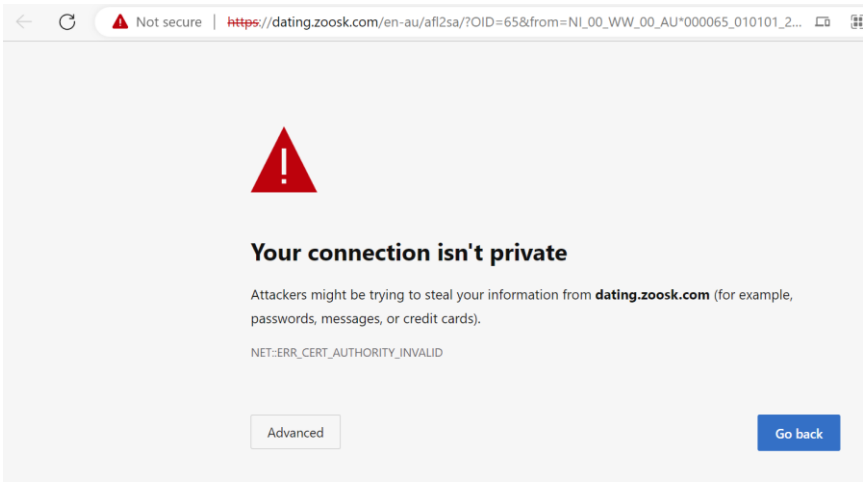
Part d.



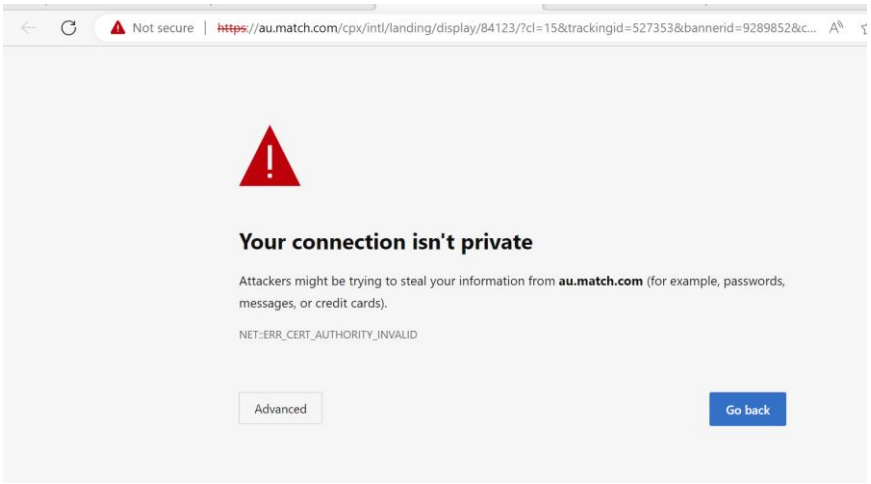
RANK	DOMAIN	REASON	REQUESTS
1	www.facebook.com	Blacklist	20
2	gateway.instagram.com	Blacklist	16
3	graph.facebook.com	Blacklist	6
4	facebook.com	Blacklist	3
5	www.eharmony.com.au	Dating	2
6	www.dating.com	Dating	2
7	bws.com.au	Alcohol	2
8	mqtt-mini.facebook.com	Blacklist	2
9	api.likee.video	Dating, ...	2
10	edge-chat.instagram.com	Blacklist	1
11	tms.eharmony.com.au	Dating	1
12	www.danmurphys.com.au	Alcohol	1

Part e.

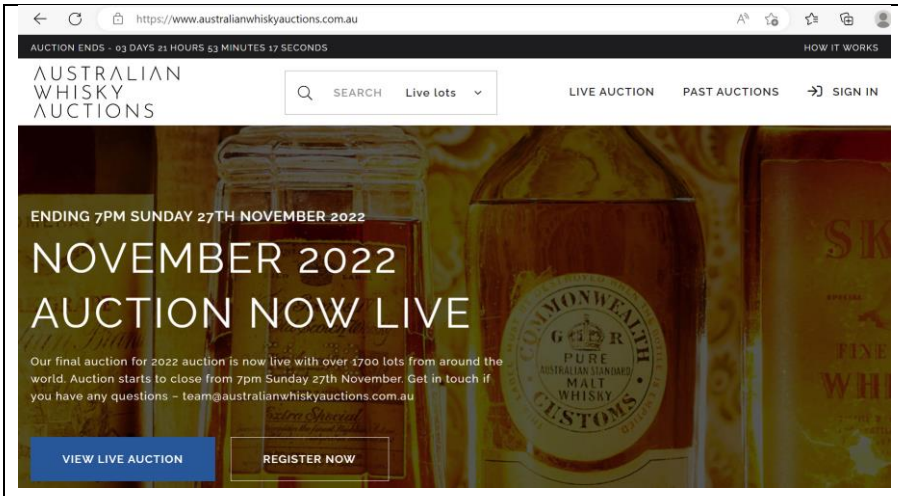
First spot check:



Second spot check:



Third spot check



OpenDNS logging

Domains

Domains for Personal Networks on 2022-11-23 or choose a range of days Apply

Filter: View only requests that were blocked

RANK	DOMAIN	REASON	REQUESTS
1	www.facebook.com	Blacklist	20
2	gateway.instagram.com	Blacklist	16
3	graph.facebook.com	Blacklist	6
4	facebook.com	Blacklist	3
5	www.eharmony.com.au	Dating	2
6	dating.zoosk.com	Dating	2
7	www.dating.com	Dating	2
8	au.match.com	Dating, ...	2
9	bws.com.au	Alcohol	2
10	mqtt-mini.facebook.com	Blacklist	2
11	www.danmurphys.com.au	Alcohol	2
12	api.likee.video	Dating, ...	2
13	edge-chat.instagram.com	Blacklist	1
14	tms.eharmony.com.au	Dating	1

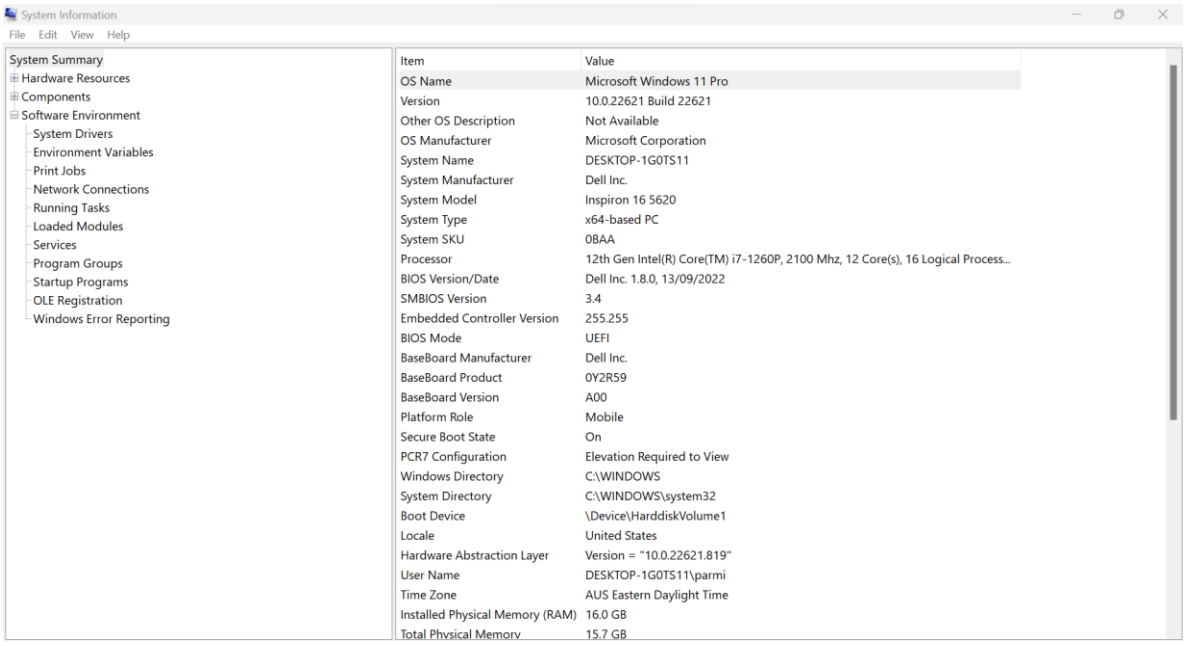
Part f:

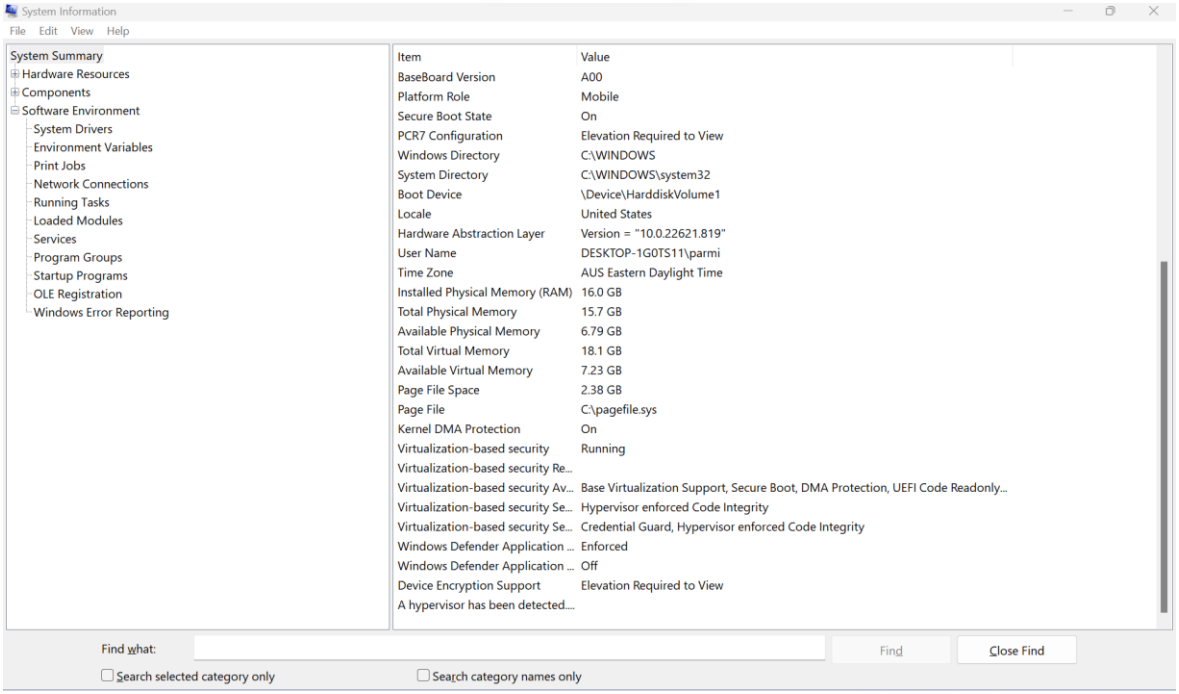
I added the https://www.australianwhiskyauctions.com.au/ to the alcohol category; it is awaiting votes.

Part g: Not yet decided in any category; awaiting votes!

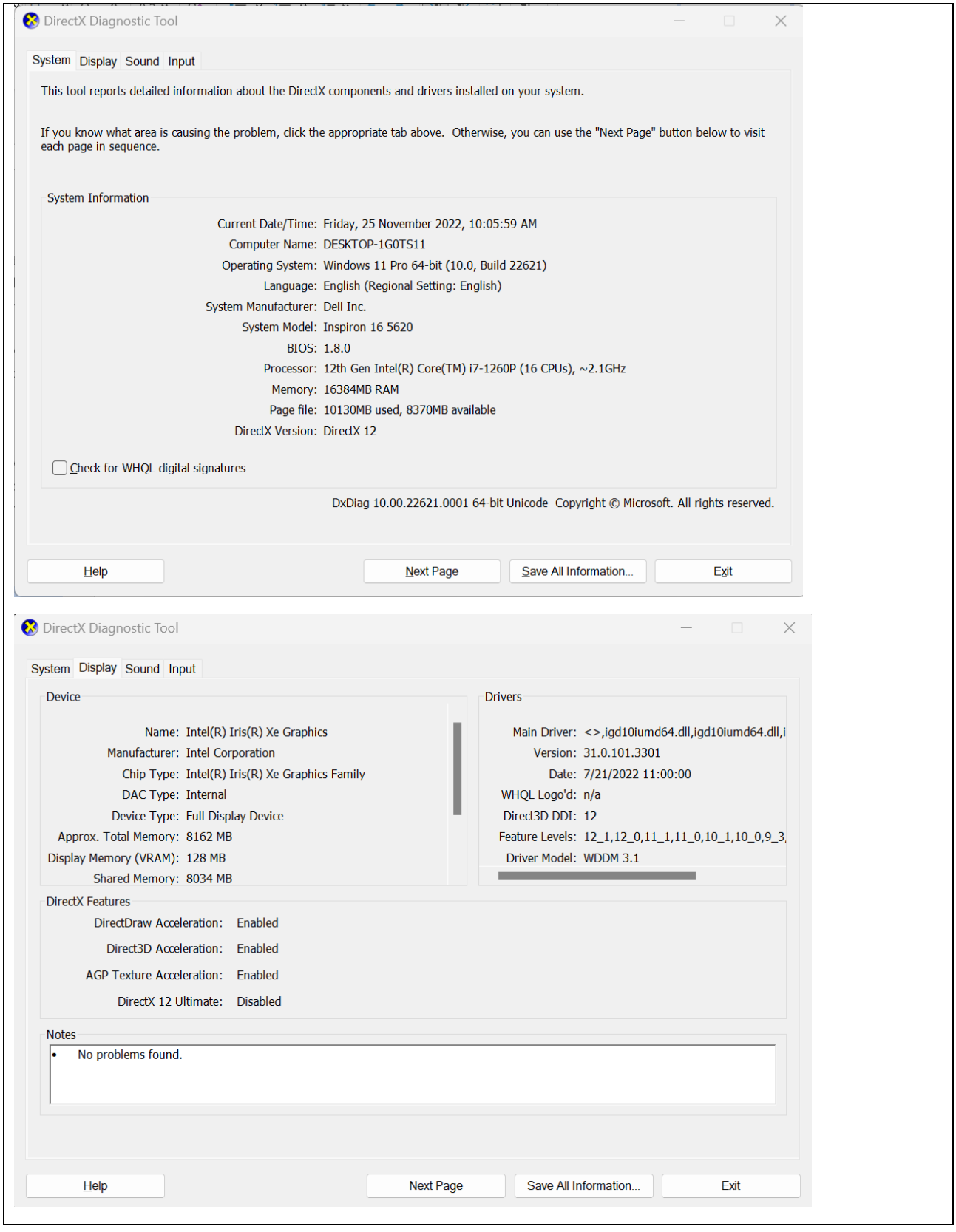
3.4 Conducting system audit

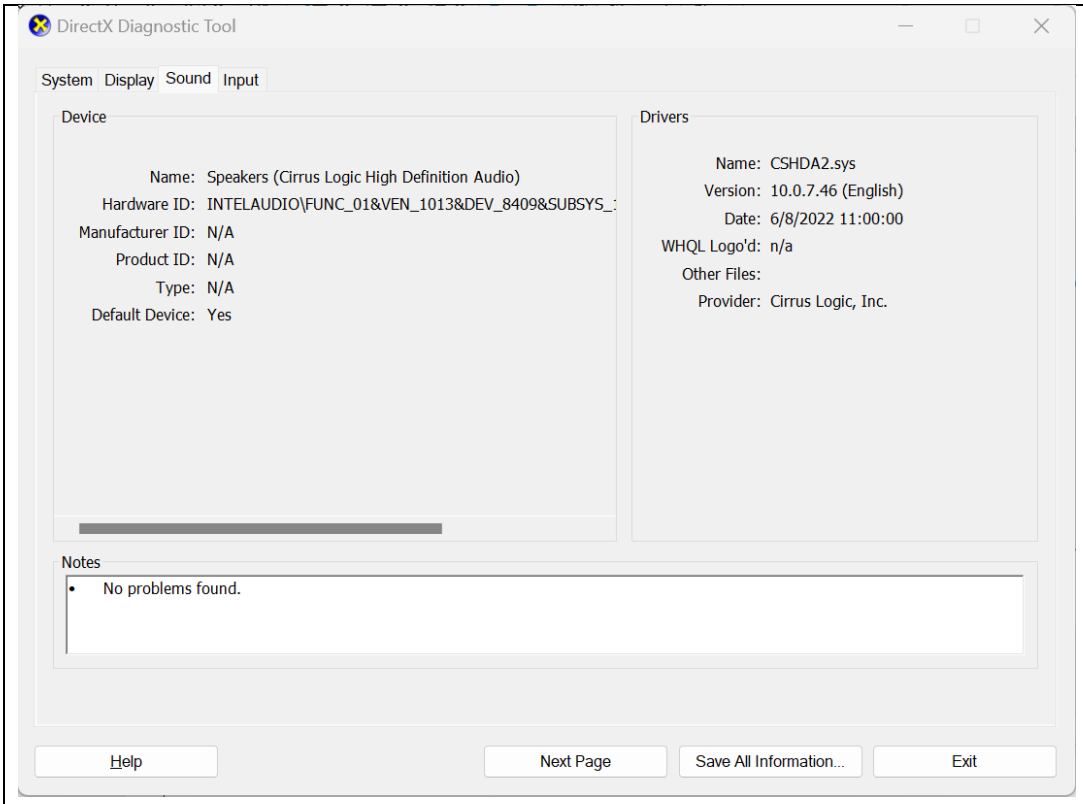
a. Screenshot/s of using the **MSINFO32** tool to obtain relevant system asset information

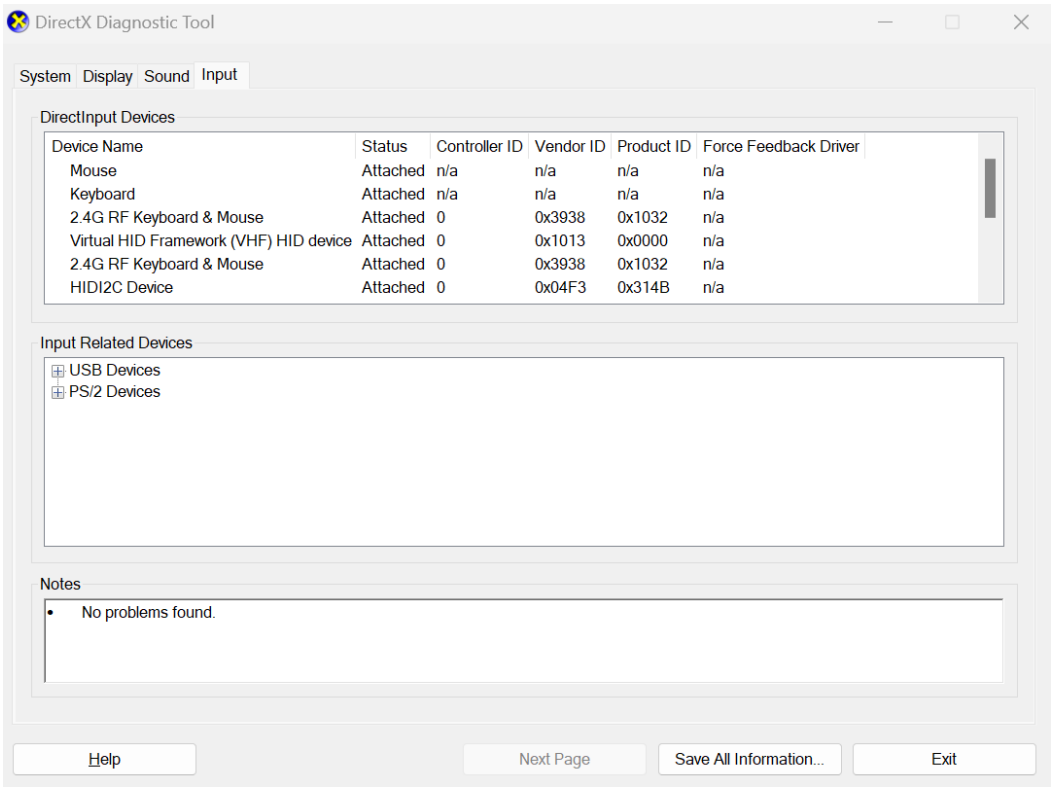




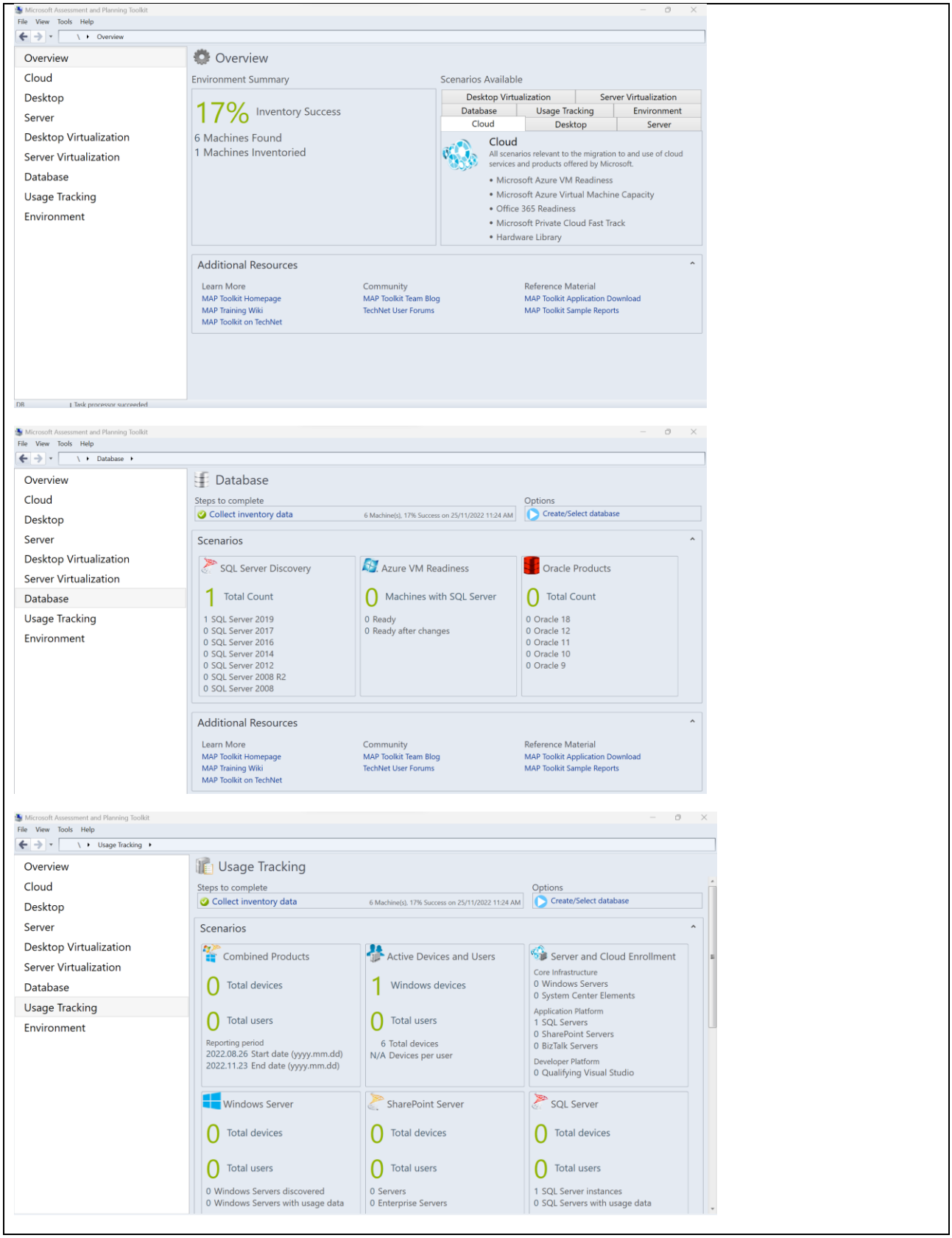
b. Screenshot/s of using the **DXdiag** tool to obtain relevant system asset information

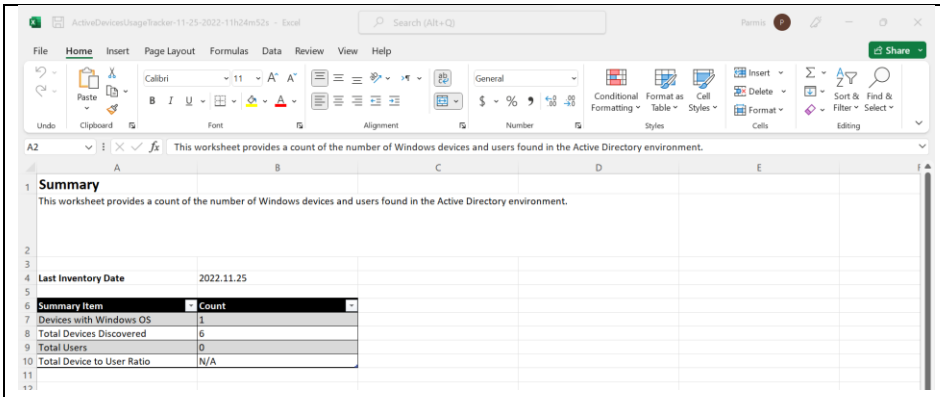

DirectX Diagnostic Tool
System Display Sound Input
This tool reports detailed information about the DirectX components and drivers installed on your system.
If you know what area is causing the problem, click the appropriate tab above. Otherwise, you can use the "Next Page" button below to visit each page in sequence.
System Information
Current Date/Time: Friday, 25 November 2022, 10:05:59 AM
Computer Name: DESKTOP-1G0TS11
Operating System: Windows 11 Pro 64-bit (10.0, Build 22621)
Language: English (Regional Setting: English)
System Manufacturer: Dell Inc.
System Model: Inspiron 16 5620
BIOS: 1.8.0
Processor: 12th Gen Intel(R) Core(TM) i7-1260P (16 CPUs), ~2.1GHz
Memory: 16384MB RAM
Page file: 10130MB used, 8370MB available
DirectX Version: DirectX 12
Check for WHQL digital signatures
DxDiag 10.00.22621.0001 64-bit Unicode Copyright © Microsoft. All rights reserved.
Help
Next Page
Save All Information...
Exit
DirectX Diagnostic Tool
System Display Sound Input
Device
Name: Intel(R) Iris(R) Xe Graphics
Manufacturer: Intel Corporation
Chip Type: Intel(R) Iris(R) Xe Graphics Family
DAC Type: Internal
Device Type: Full Display Device
Approx. Total Memory: 8162 MB
Display Memory (VRAM): 128 MB
Shared Memory: 8034 MB
Drivers
Main Driver: <>,igd10iumd64.dll,igd10iumd64.dll,i
Version: 31.0.101.3301
Date: 7/21/2022 11:00:00
WHQL Logo'd: n/a
Direct3D DDI: 12
Feature Levels: 12_1,12_0,11_1,11_0,10_1,10_0,9_3,
Driver Model: WDDM 3.1
DirectX Features
DirectDraw Acceleration: Enabled
Direct3D Acceleration: Enabled
AGP Texture Acceleration: Enabled
DirectX 12 Ultimate: Disabled
Notes
No problems found.
Help
Next Page
Save All Information...
Exit





c. Screenshot/s of using the **MAP Toolkit** to obtain relevant system asset information


Microsoft Assessment and Planning Toolkit
File View Tools Help
Overview
Cloud
Desktop
Server
Desktop Virtualization
Server Virtualization
Database
Usage Tracking
Environment
Overview
Environment Summary
17% Inventory Success
6 Machines Found
1 Machines Inventoried
Scenarios Available
Desktop Virtualization
Server Virtualization
Database
Usage Tracking
Environment
Cloud
Desktop
Server
Cloud
All scenarios relevant to the migration to and use of cloud services and products offered by Microsoft.
• Microsoft Azure VM Readiness
• Microsoft Azure Virtual Machine Capacity
• Office 365 Readiness
• Microsoft Private Cloud Fast Track
• Hardware Library
Additional Resources
Learn More
MAP Toolkit Homepage
MAP Training Wiki
MAP Toolkit on TechNet
Community
MAP Toolkit Team Blog
TechNet User Forums
Reference Material
MAP Toolkit Application Download
MAP Toolkit Sample Reports
Database
Steps to complete
Collect inventory data
6 Machine(s), 17% Success on 25/11/2022 11:24 AM
Options
Create/Select database
Scenarios
SQL Server Discovery
1 Total Count
1 SQL Server 2019
0 SQL Server 2017
0 SQL Server 2016
0 SQL Server 2014
0 SQL Server 2012
0 SQL Server 2008 R2
0 SQL Server 2008
Azure VM Readiness
0 Machines with SQL Server
0 Ready
0 Ready after changes
Oracle Products
0 Total Count
0 Oracle 18
0 Oracle 12
0 Oracle 11
0 Oracle 10
0 Oracle 9
Usage Tracking
Steps to complete
Collect inventory data
6 Machine(s), 17% Success on 25/11/2022 11:24 AM
Options
Create/Select database
Scenarios
Combined Products
0 Total devices
0 Total users
Reporting period
2022.08.26 Start date (yyyy.mm.dd)
2022.11.23 End date (yyyy.mm.dd)
Active Devices and Users
1 Windows devices
0 Total users
6 Total devices
N/A Devices per user
Server and Cloud Enrollment
Core Infrastructure
0 Windows Servers
0 System Center Elements
Application Platform
1 SQL Servers
0 SharePoint Servers
0 BizTalk Servers
Developer Platform
0 Qualifying Visual Studio
Windows Server
0 Total devices
0 Total users
0 Windows Servers discovered
0 Windows Servers with usage data
SharePoint Server
0 Total devices
0 Total users
0 Servers
0 Enterprise Servers
SQL Server
0 Total devices
0 Total users
1 SQL Server instances
0 SQL Servers with usage data



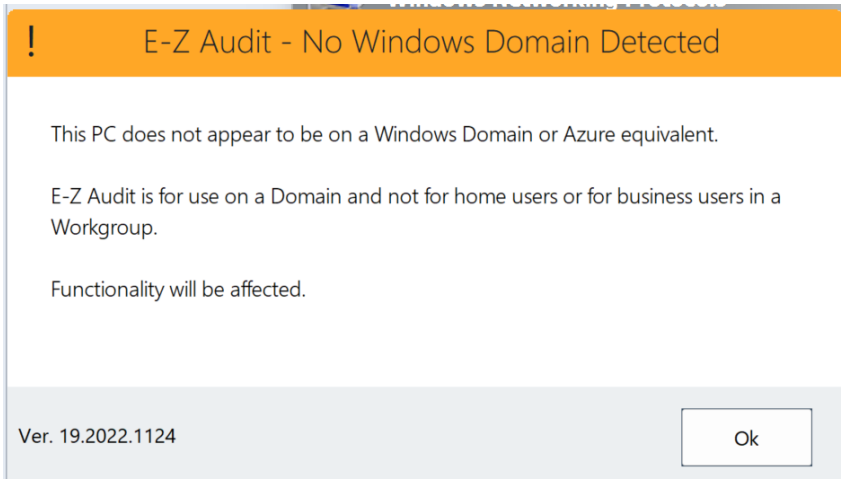
Summary

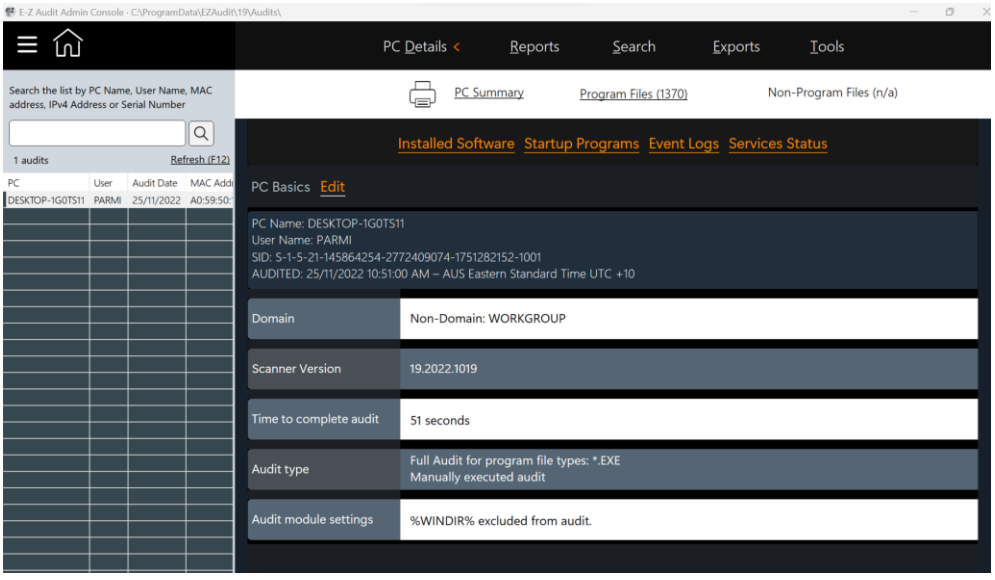
This worksheet provides a count of the number of Windows devices and users found in the Active Directory environment.

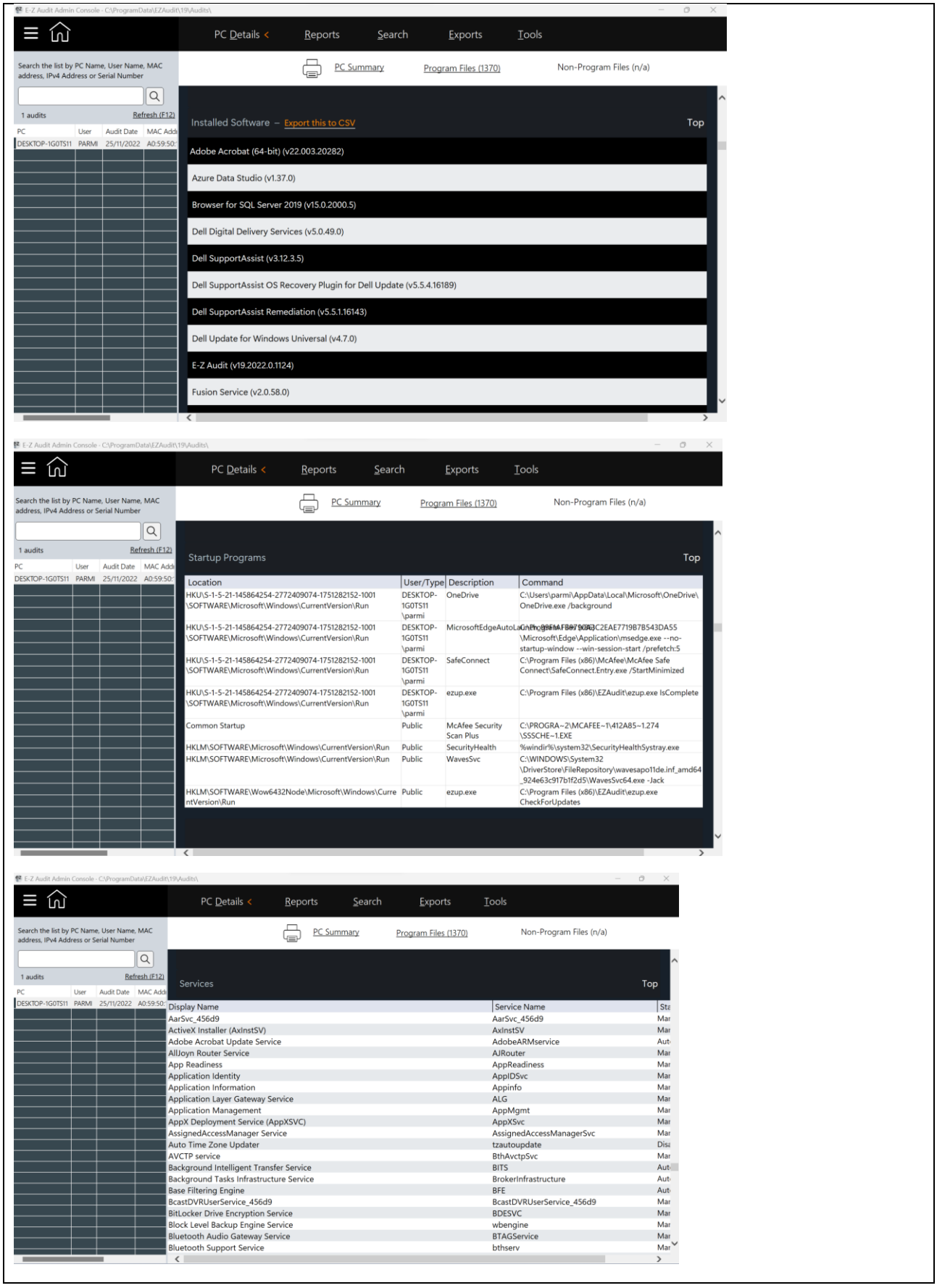
Last Inventory Date	2022.11.25

Summary Item	Count
Devices with Windows OS	1
Total Devices Discovered	6
Total Users	0
Total Device to User Ratio	N/A

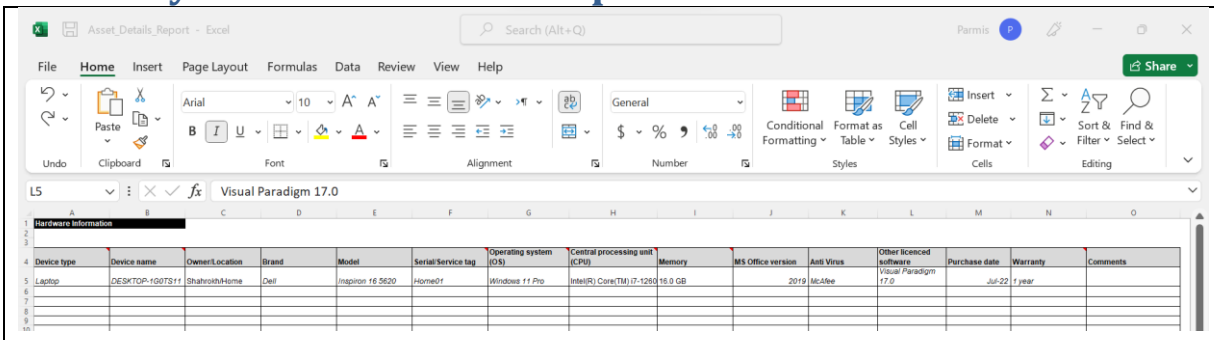
d. Screenshot/s of using the **E-Z Audit** tool to obtain relevant system asset information.



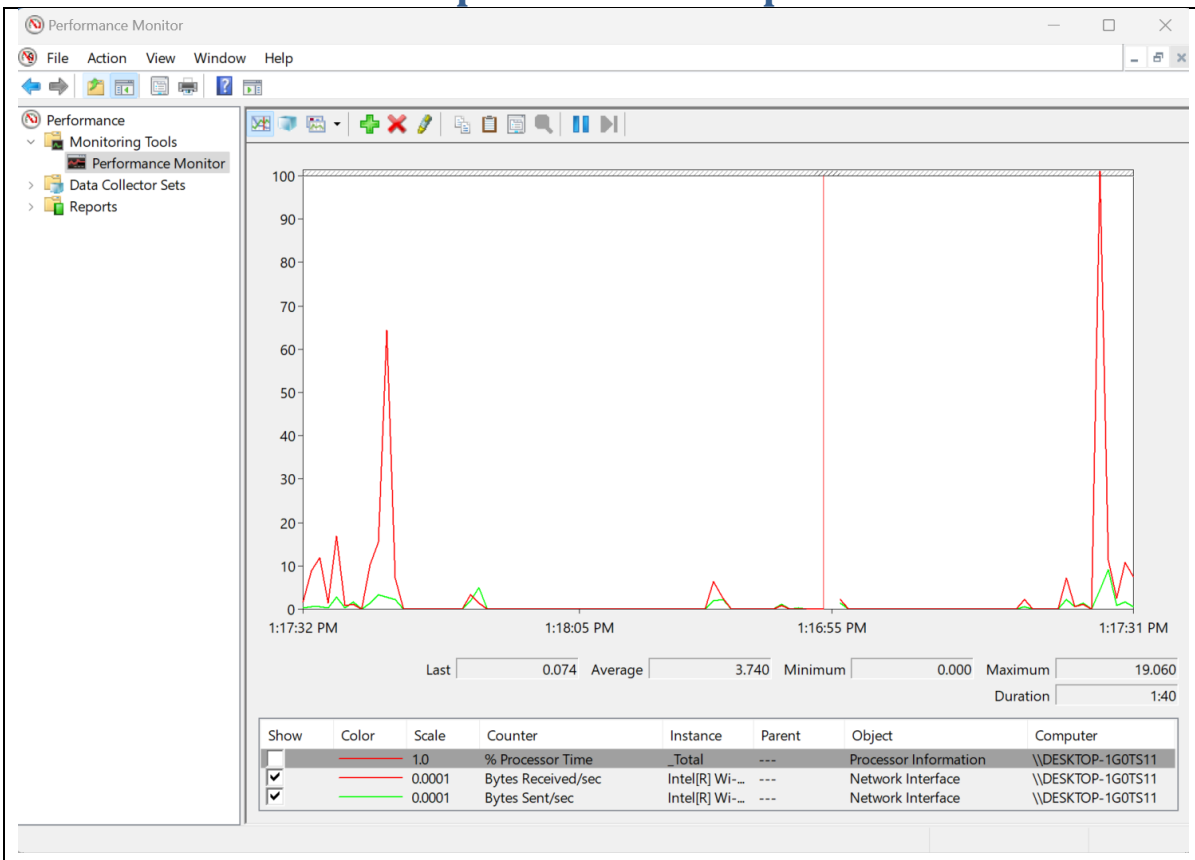



E-Z Audit Admin Console - C:\ProgramData\EZAudit\19\Audits\
PC Details
Reports
Search
Exports
Tools
Search the list by PC Name, User Name, MAC address, IPv4 Address or Serial Number
1 audits
Refresh (F12)
PC
User
Audit Date
MAC Addi
DESKTOP-1G0TS11
PARMI
25/11/2022
A0:59:50:
PC Summary
Program Files (1370)
Non-Program Files (n/a)
Installed Software – Export this to CSV
Top
Adobe Acrobat (64-bit) (v22.003.20282)
Azure Data Studio (v1.37.0)
Browser for SQL Server 2019 (v15.0.2000.5)
Dell Digital Delivery Services (v5.0.49.0)
Dell SupportAssist (v3.12.3.5)
Dell SupportAssist OS Recovery Plugin for Dell Update (v5.5.4.16189)
Dell SupportAssist Remediation (v5.5.1.16143)
Dell Update for Windows Universal (v4.7.0)
E-Z Audit (v19.2022.0.1124)
Fusion Service (v2.0.58.0)
Startup Programs
Top
Location
User/Type
Description
Command
HKU\S-1-5-21-145864254-2772409074-1751282152-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
DESKTOP-1G0TS11\parmi
OneDrive
C:\Users\parmi\AppData\Local\Microsoft\OneDrive\OneDrive.exe /background
HKU\S-1-5-21-145864254-2772409074-1751282152-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
DESKTOP-1G0TS11\parmi
MicrosoftEdgeAutoLaunch_
C2EAE7719B7B543DA55
\Microsoft\Edge\Application\msedge.exe --no-startup-window --win-session-start /prefetch:5
HKU\S-1-5-21-145864254-2772409074-1751282152-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
DESKTOP-1G0TS11\parmi
SafeConnect
C:\Program Files (x86)\McAfee\McAfee Safe Connect\SafeConnect.Entry.exe /StartMinimized
HKU\S-1-5-21-145864254-2772409074-1751282152-1001\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
DESKTOP-1G0TS11\parmi
ezup.exe
C:\Program Files (x86)\EZAudit\ezup.exe IsComplete
Common Startup
Public
McAfee Security Scan Plus
C:\PROGRA~2\MCAFEE~1\412A85~1.274\SSSCHE~1.EXE
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
Public
SecurityHealth
%windir%\system32\SecurityHealthSystray.exe
HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Run
Public
WavesSvc
C:\WINDOWS\System32\DriverStore\FileRepository\wavesapo11de.inf_amd64_924e63c917b1f2d5\WavesSvc64.exe -Jack
HKLM\SOFTWARE\Wow6432Node\Microsoft\Windows\CurrentVersion\Run
Public
ezup.exe
C:\Program Files (x86)\EZAudit\ezup.exe CheckForUpdates
Services
Top
Display Name
Service Name
AarSvc_456d9
ActiveX Installer (AxInstSV)
Adobe Acrobat Update Service
AllJoyn Router Service
App Readiness
Application Identity
Application Information
Application Layer Gateway Service
Application Management
AppX Deployment Service (AppXSVC)
AssignedAccessManager Service
Auto Time Zone Updater
AVCTP service
Background Intelligent Transfer Service
Background Tasks Infrastructure Service
Base Filtering Engine
BcastDVRUserService_456d9
BitLocker Drive Encryption Service
Block Level Backup Engine Service
Bluetooth Audio Gateway Service
Bluetooth Support Service
AarSvc_456d9
AxInstSV
AdobeARMservice
AJRouter
AppReadiness
AppIDSvc
Appinfo
ALG
AppMgmt
AppXSvc
AssignedAccessManagerSvc
tzautoupdate
BthAvctpSvc
BITS
BrokerInfrastructure
BFE
BcastDVRUserService_456d9
BDESVC
wbengine
BTAGService
bthserv

3.5 System asset details report



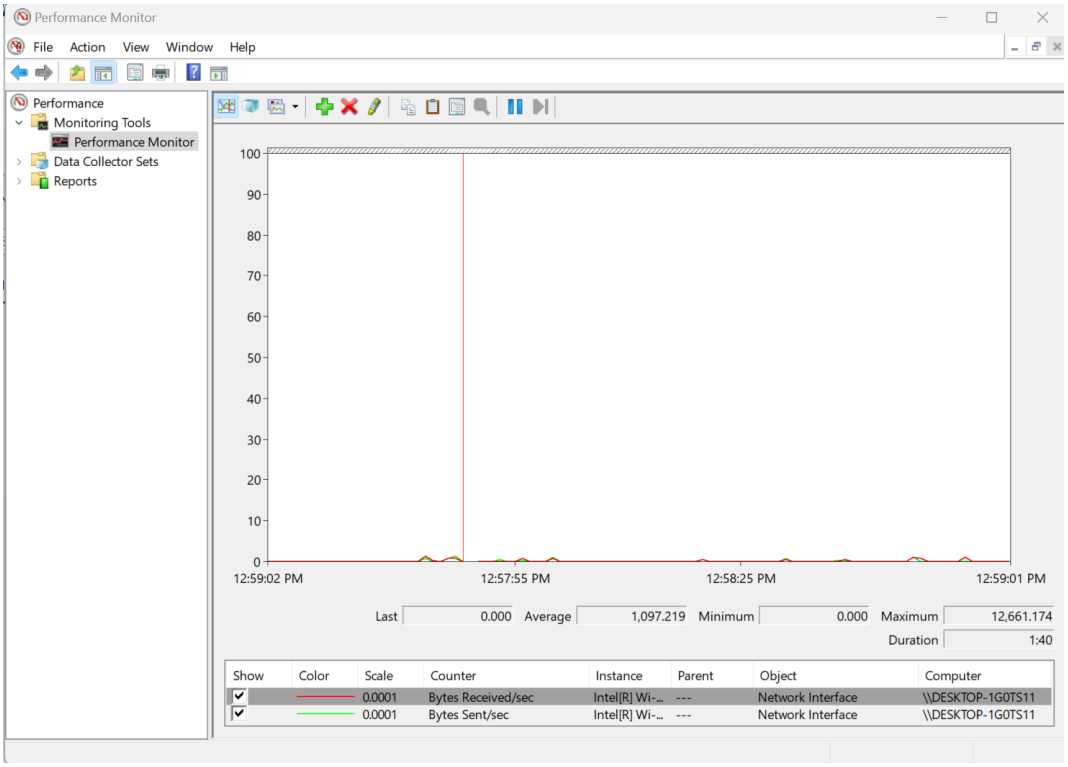
3.6 Network traffic performance report



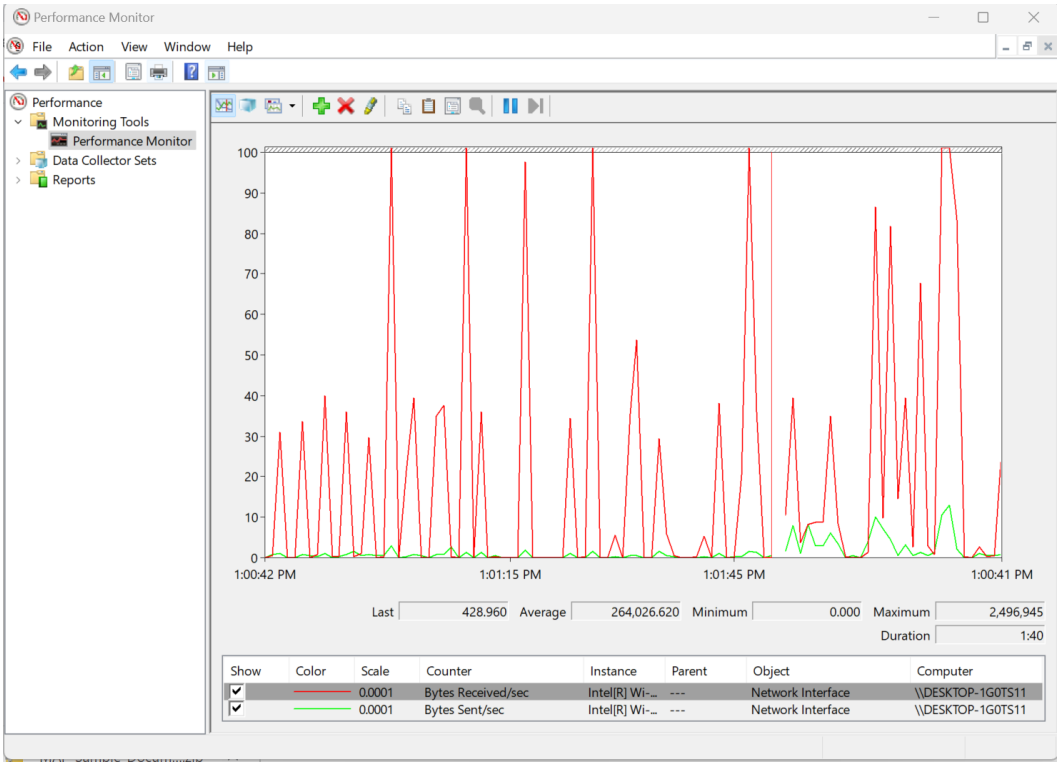
1. Type "**performance monitor**" in the search field located on the taskbar.
2. Click on the **Performance Monitor** shortcut to open it.
3. Now, from the left pane, select '**Performance Monitor**' under '**Monitoring Tools**'.
4. Click on the **green plus shaped icon** on top of the graph.
5. Select the name of the computer in the '**Select counters from computer**' drop-down menu.
6. Now, expand the category of **Network Interface.**
7. Select **Bytes Received/sec** and **Bytes Sent/sec** from the list.
8. Click on **Add button** to add the counters. The added counters will be shown on the right side.

9. Click on OK to confirm.

Expectation for low network loads:



Expectation for high network load



4. Design and implement security system

4.1 Network scan results

a. I used Nmap

Router

```
C:\Users\parmi>nmap 192.168.1.1
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-27 20:44 AUS Eastern Daylight Time
Nmap scan report for 192-168-1-1.tpgi.com.au (192.168.1.1)
Host is up (0.0039s latency).
Not shown: 993 closed tcp ports (reset)
PORT     STATE SERVICE
21/tcp   open  ftp
53/tcp   open  domain
80/tcp   open  http
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
1900/tcp open  upnp
8200/tcp open  trivnet1
MAC Address: 34:E8:94:33:E1:B2 (Tp-link Technologies)

Nmap done: 1 IP address (1 host up) scanned in 8.00 seconds
```

Laptop

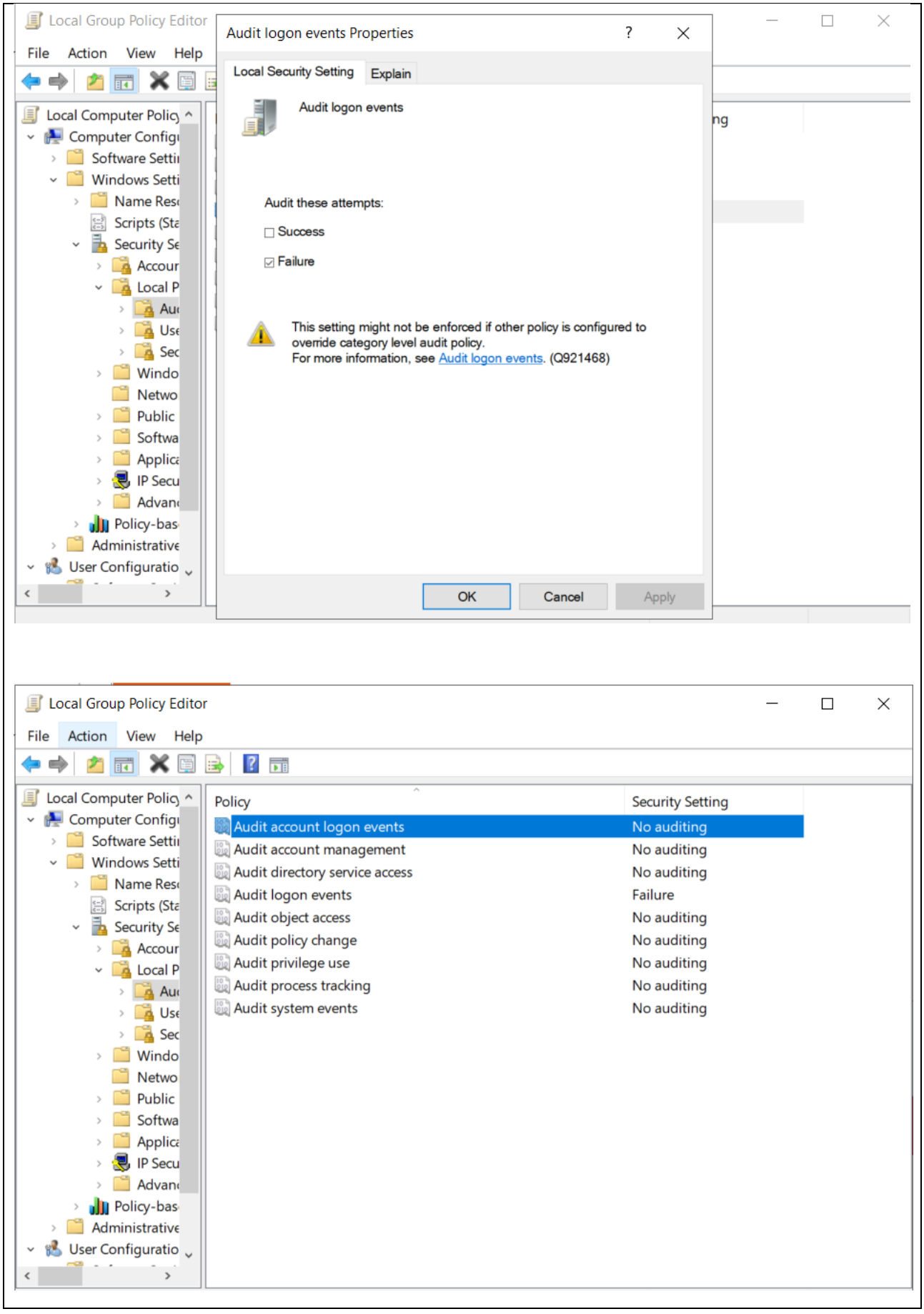
```
C:\Users\parmi>nmap 192.168.1.107
Starting Nmap 7.93 ( https://nmap.org ) at 2022-11-27 20:46 AUS Eastern Daylight Time
Nmap scan report for 192-168-1-107.tpgi.com.au (192.168.1.107)
Host is up (0.0014s latency).
Not shown: 996 closed tcp ports (reset)
PORT     STATE SERVICE
135/tcp  open  msrpc
139/tcp  open  netbios-ssn
445/tcp  open  microsoft-ds
6646/tcp open  unknown

Nmap done: 1 IP address (1 host up) scanned in 6.09 seconds
```

b.

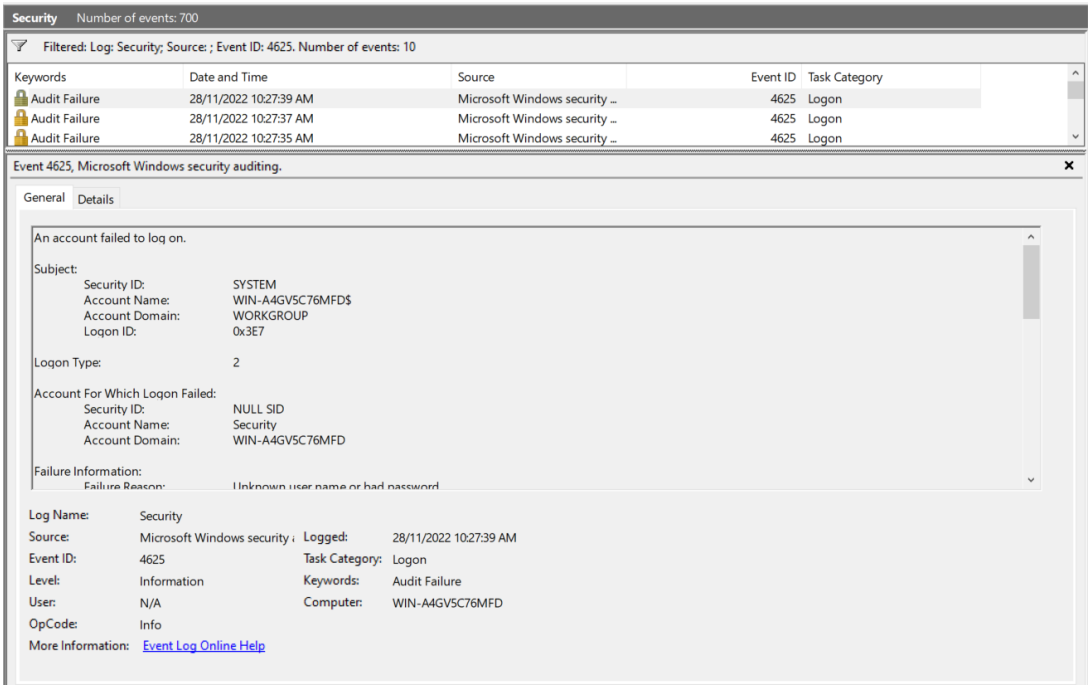
1. Open the command prompt.
2. Type **nmap [ip_address]** to initiate a default scan.

4.2 System audit results

a. First, we should enable logon event auditing in gpedit.msc

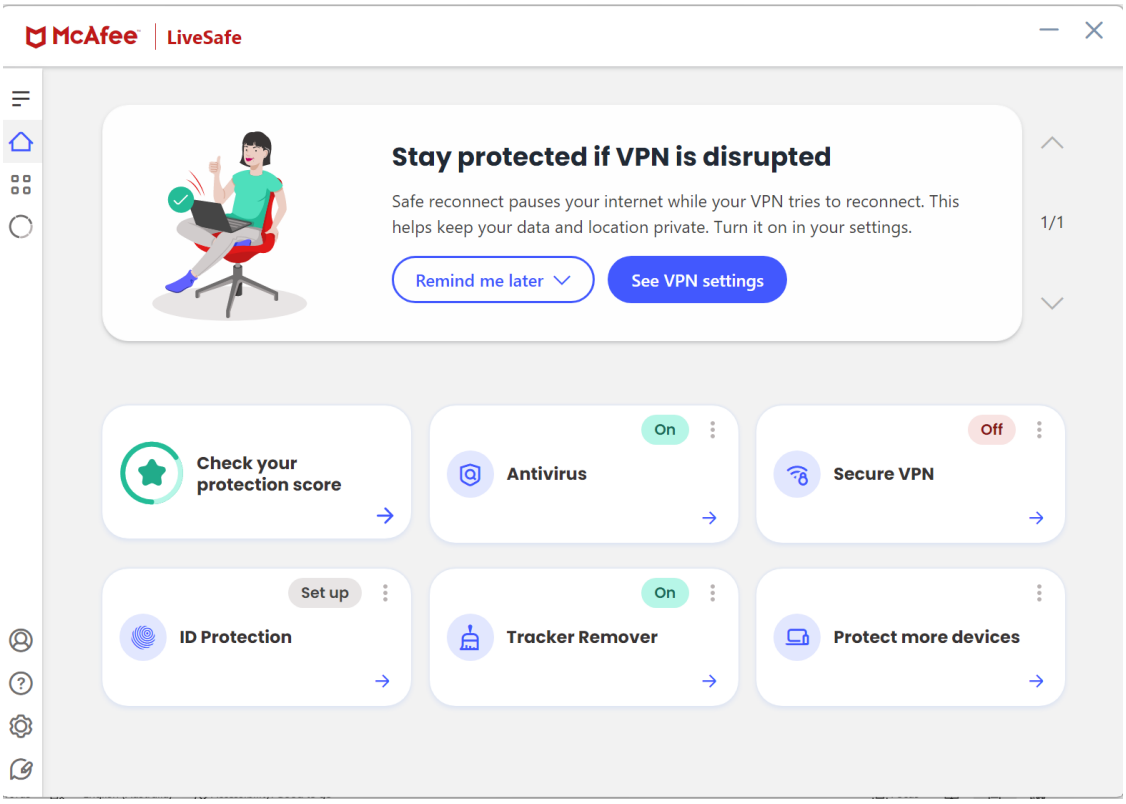

Local Group Policy Editor
File Action View Help
Audit logon events Properties
Local Security Setting
Explain
Audit logon events
Audit these attempts:
Success
Failure
This setting might not be enforced if other policy is configured to override category level audit policy.
For more information, see Audit logon events. (Q921468)
OK
Cancel
Apply
Local Group Policy Editor
File Action View Help
Policy
Security Setting
Audit account logon events
No auditing
Audit account management
No auditing
Audit directory service access
No auditing
Audit logon events
Failure
Audit object access
No auditing
Audit policy change
No auditing
Audit privilege use
No auditing
Audit process tracking
No auditing
Audit system events
No auditing

b. After three unsuccessful logons, we can audit it in event viewer.

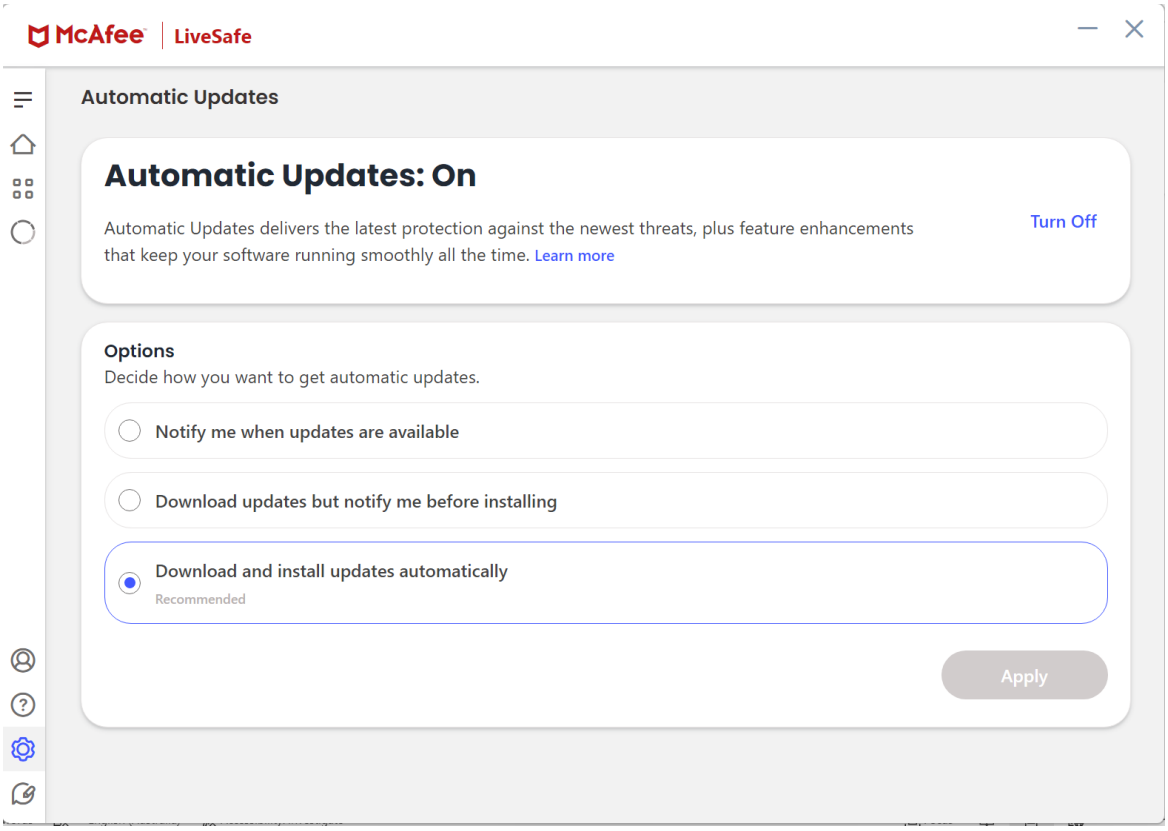


4.3 Antivirus and anti-malware solution

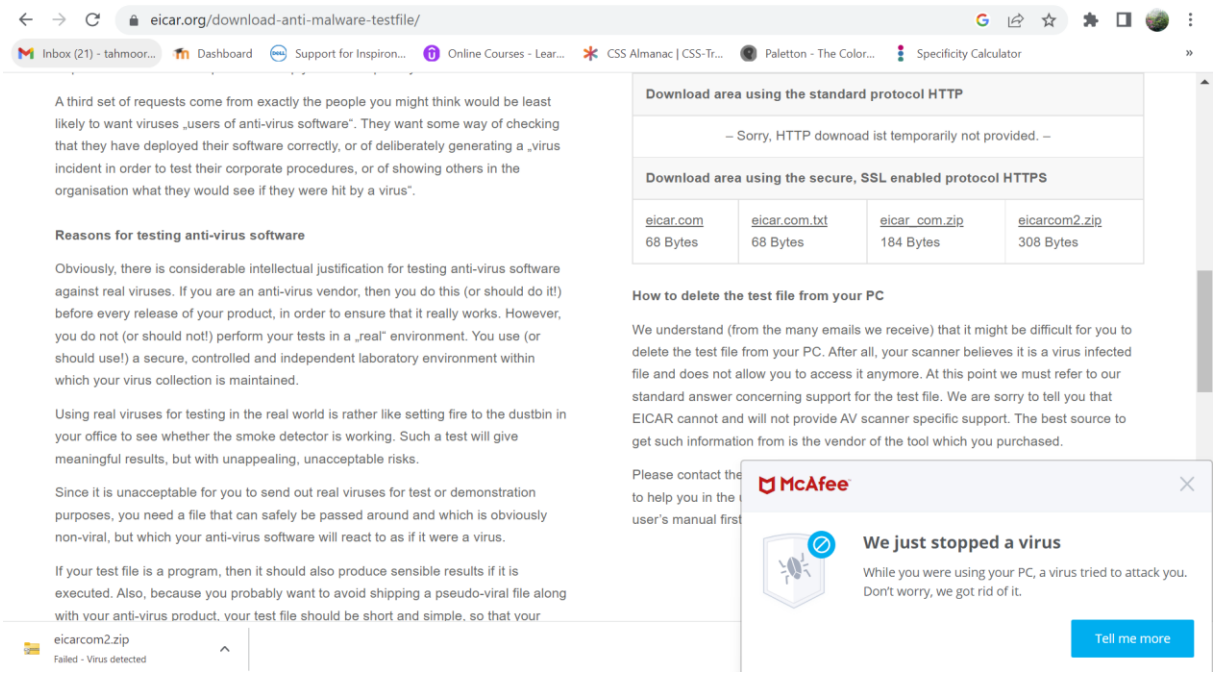
a. Installation/activation of the anti-virus / anti-malware software according to vendor specifications



b. Updating the anti-virus software with the latest virus definitions

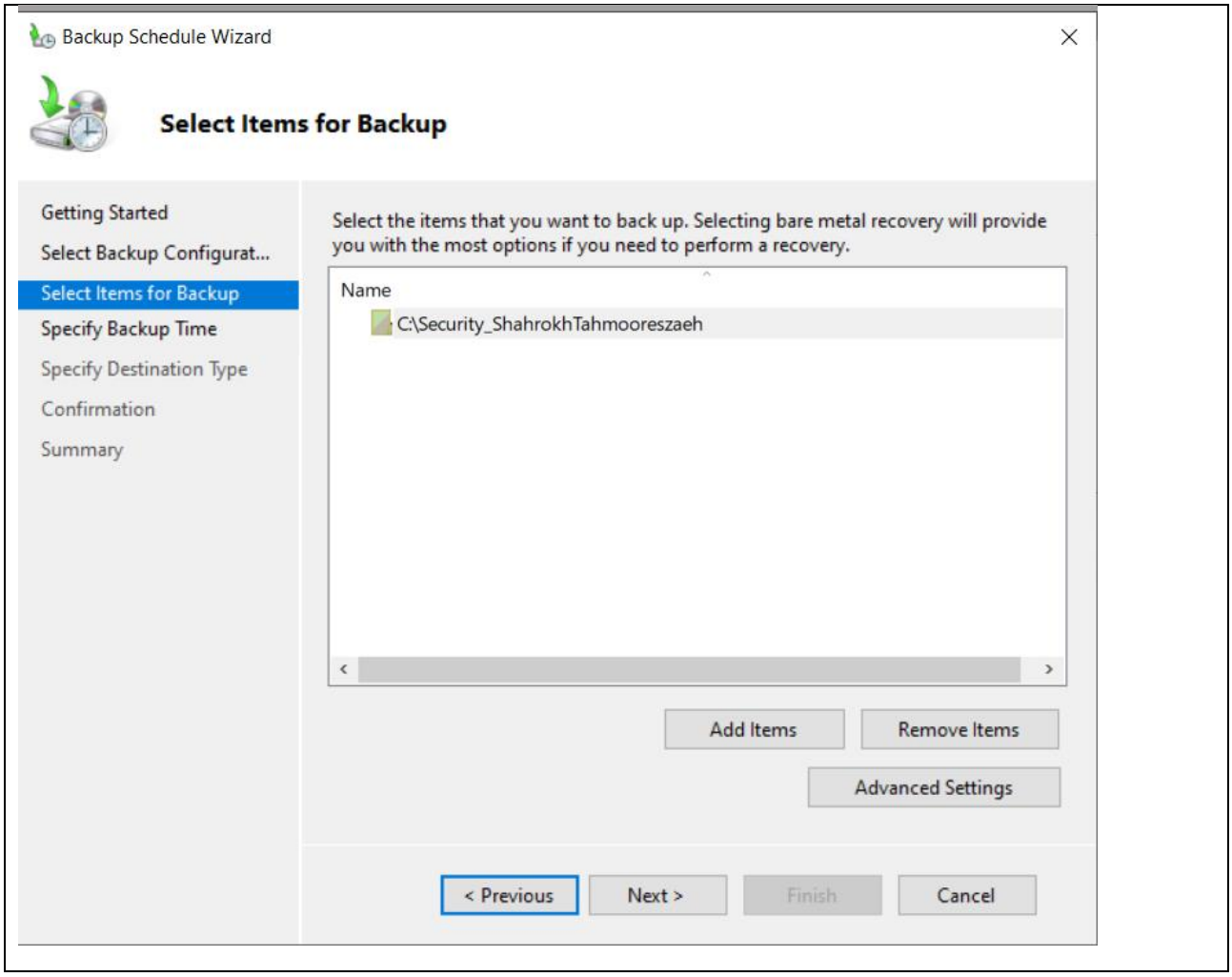


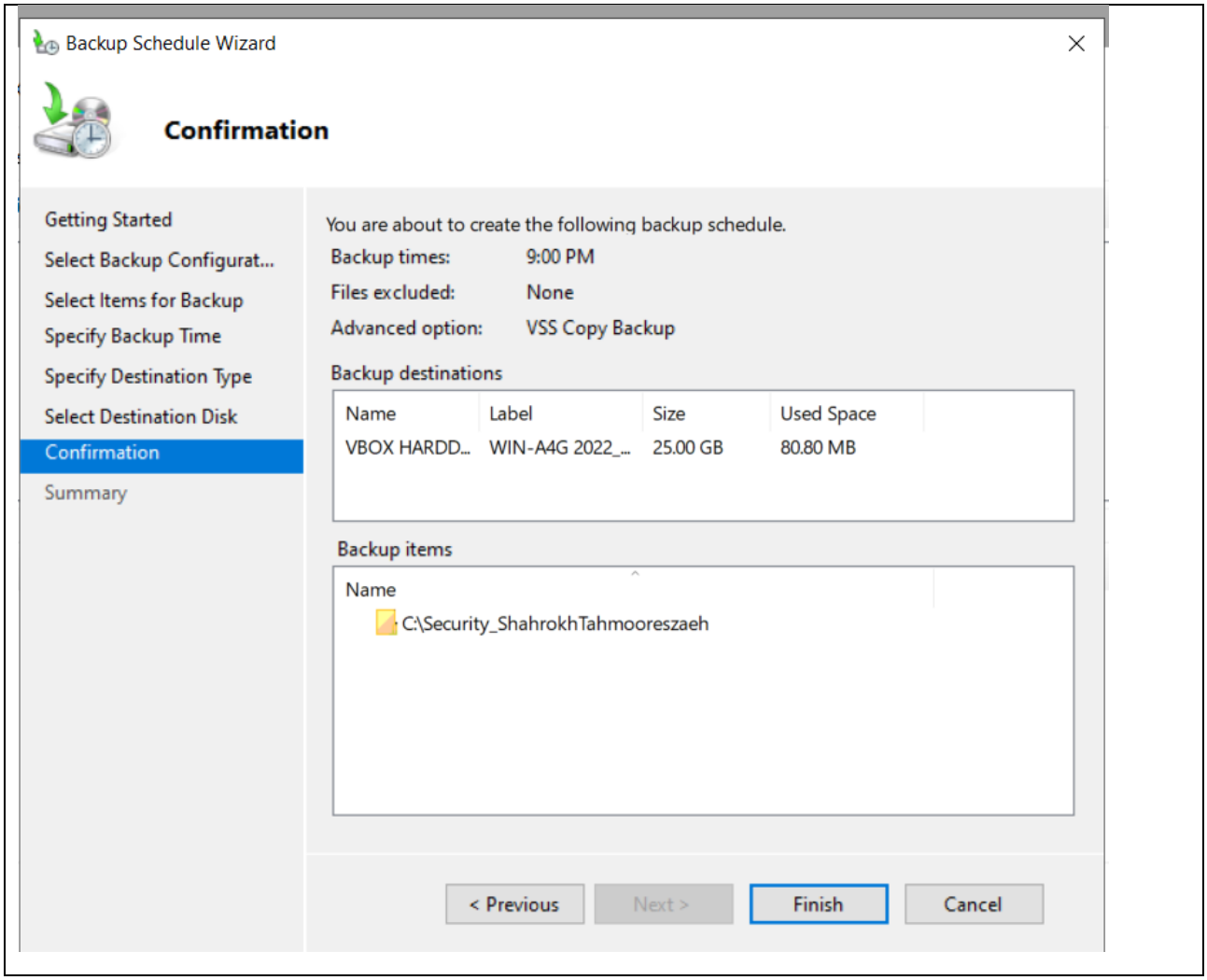
c. Testing the software for correct functionality

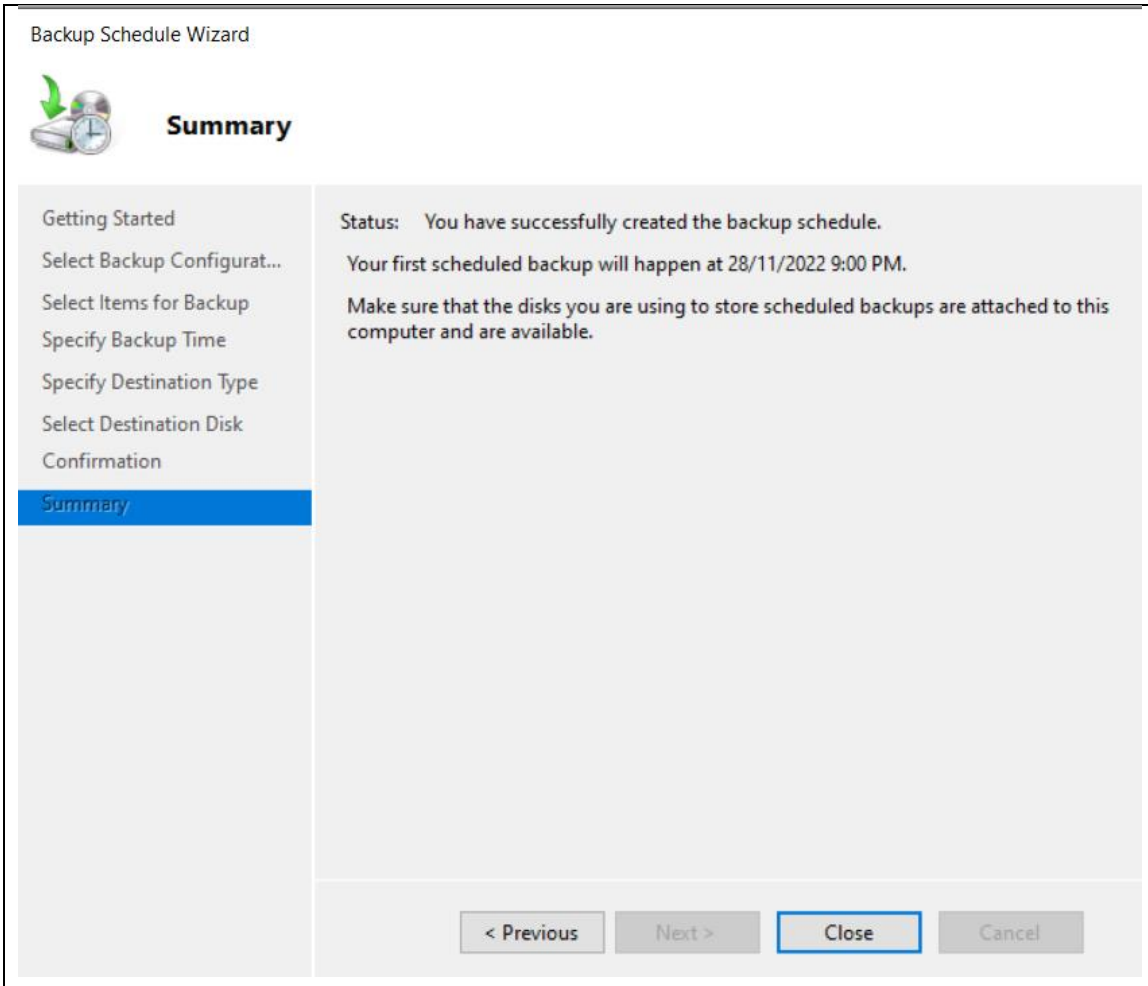


4.4 Data backup and sync solution to protect from environmental threats

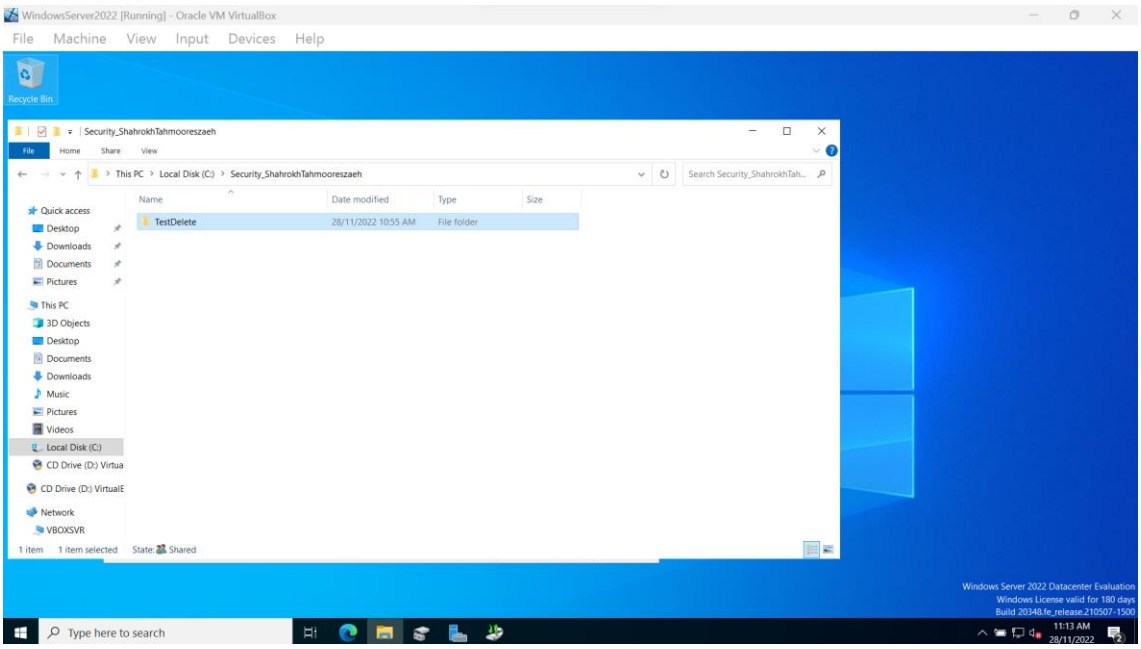
a. Evidence of carrying out a data backup in the current system


Backup Schedule Wizard
Select Items for Backup
Getting Started
Select Backup Configurat...
Select Items for Backup
Specify Backup Time
Specify Destination Type
Confirmation
Summary
Select the items that you want to back up. Selecting bare metal recovery will provide you with the most options if you need to perform a recovery.
Name
C:\Security_ShahrokhTahmooreszaeh
Add Items
Remove Items
Advanced Settings
< Previous
Next >
Finish
Cancel

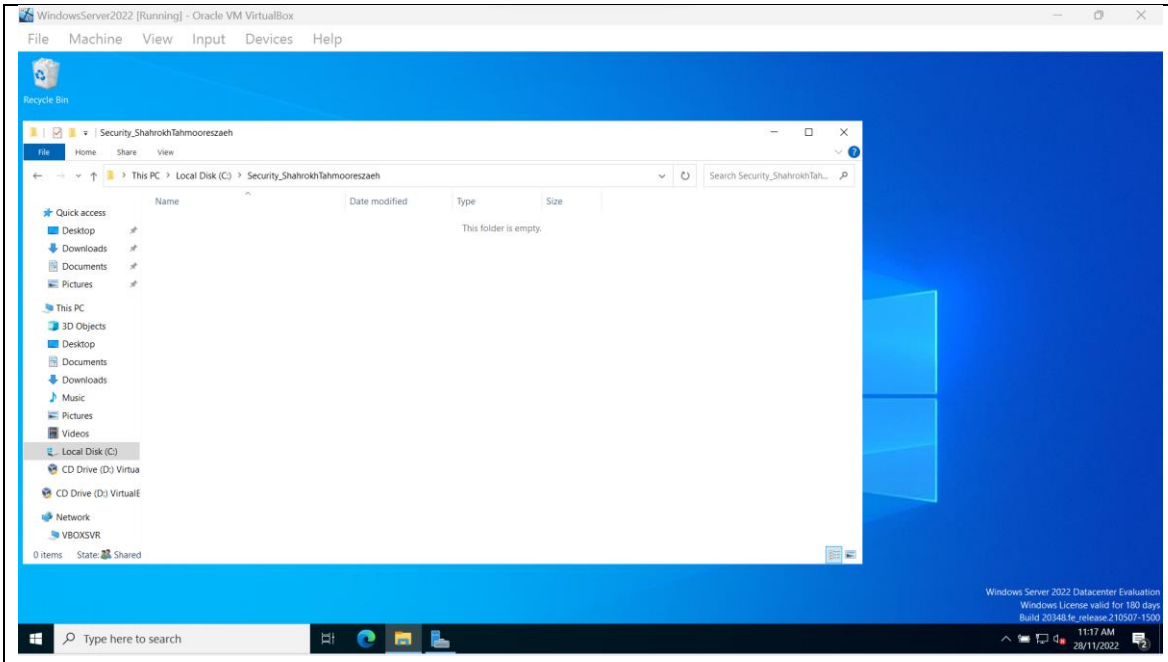

Backup Schedule Wizard
Confirmation
Getting Started
Select Backup Configurat...
Select Items for Backup
Specify Backup Time
Specify Destination Type
Select Destination Disk
Confirmation
Summary
You are about to create the following backup schedule.
Backup times: 9:00 PM
Files excluded: None
Advanced option: VSS Copy Backup
Backup destinations
Name Label Size Used Space
VBOX HARDD... WIN-A4G 2022_... 25.00 GB 80.80 MB
Backup items
Name
C:\Security_ShahrokhTahmooreszaeh
< Previous
Next >
Finish
Cancel



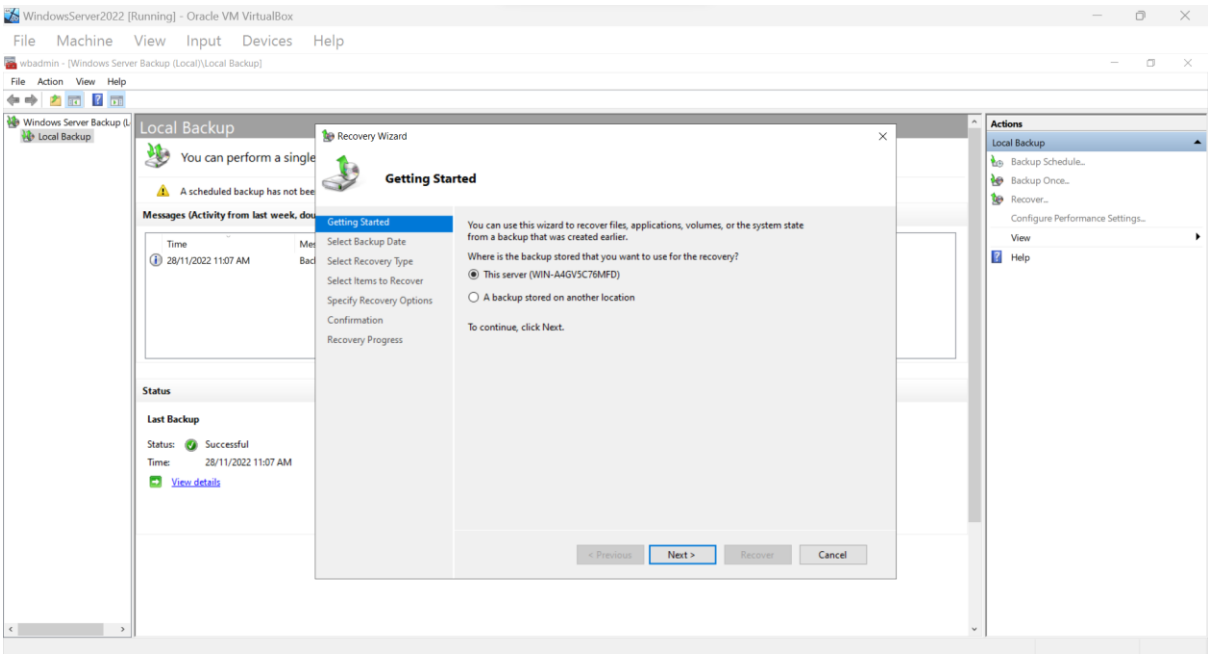
b. Screenshot/s showing data (folder) restore procedure from backup

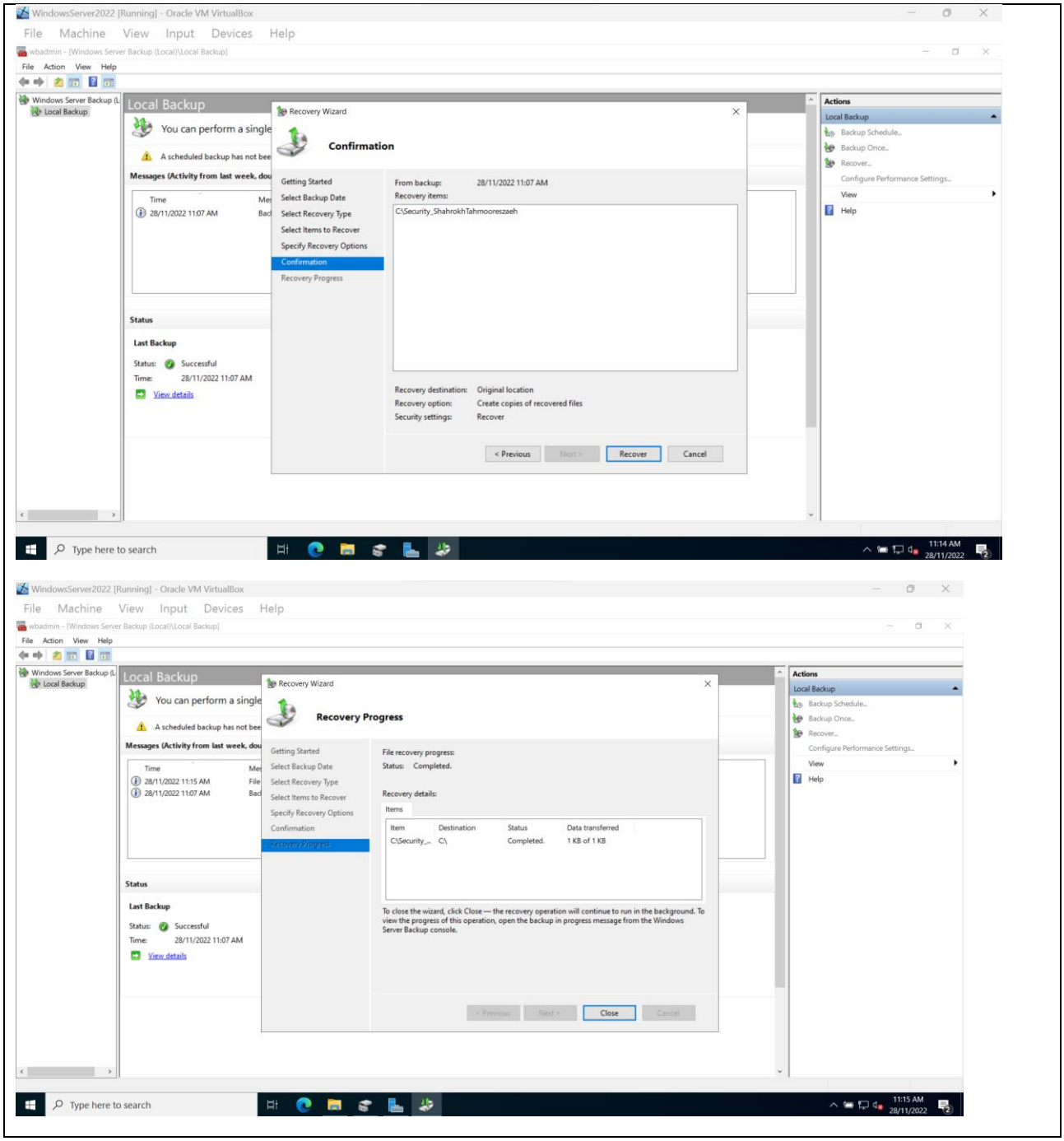


Deleting the folder:

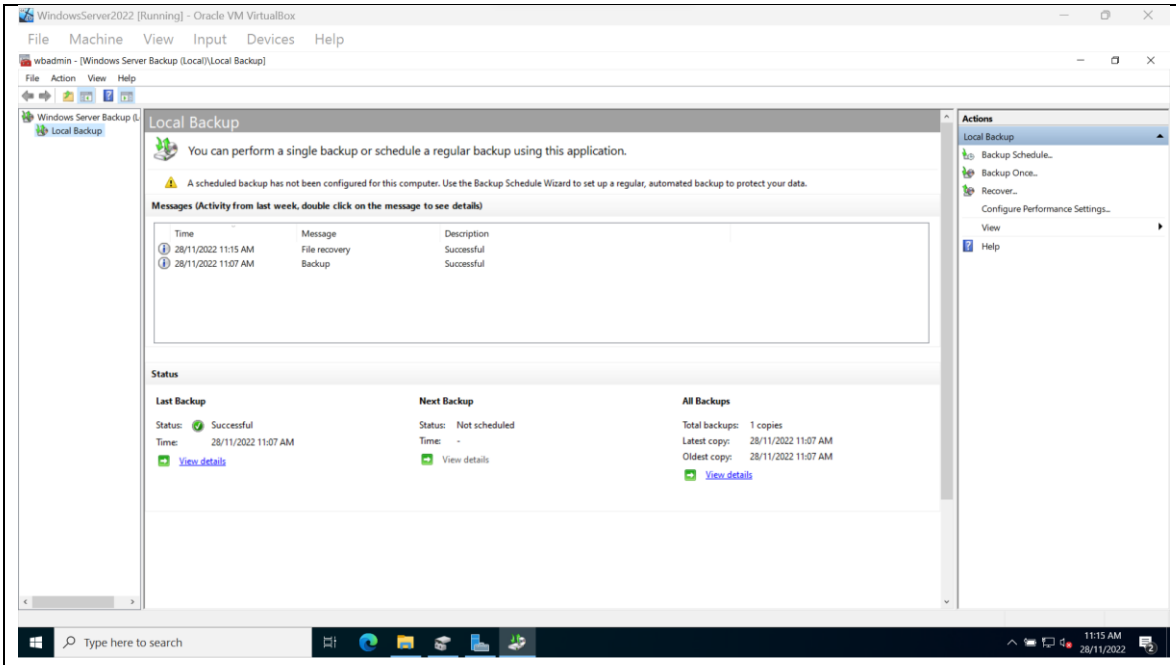


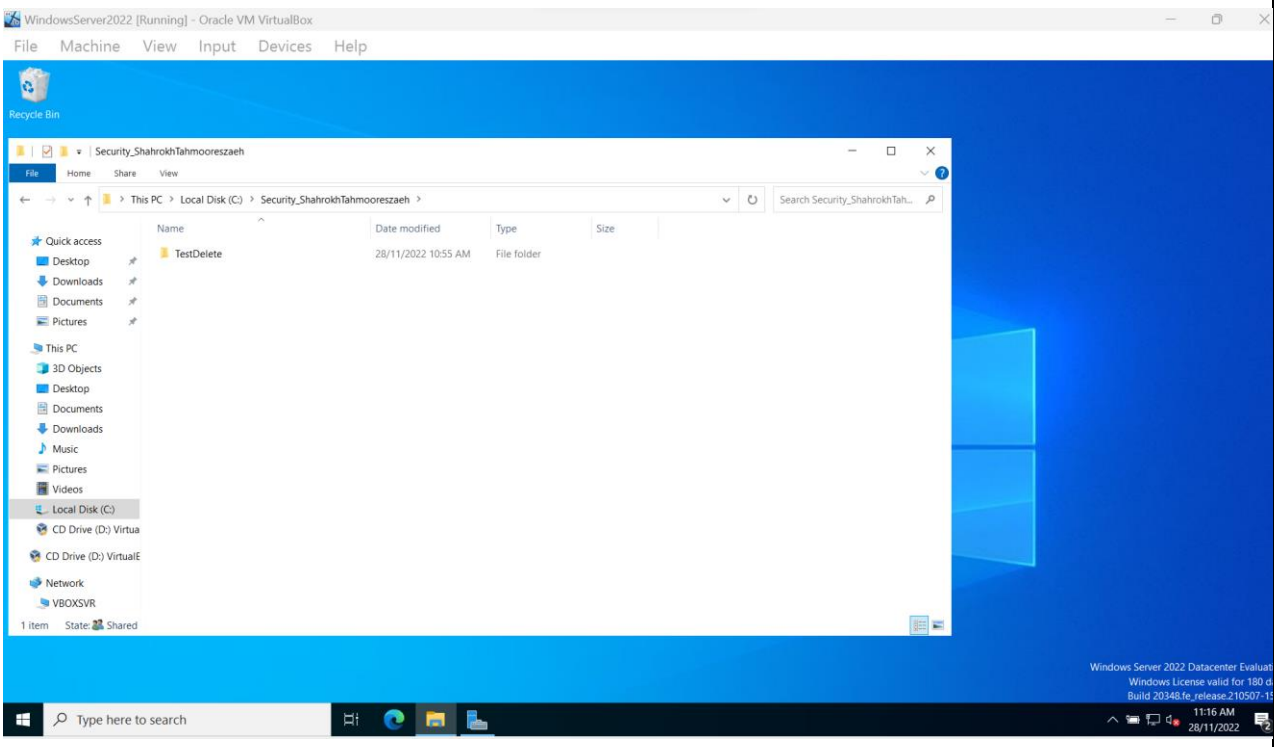
Restoring the folder:



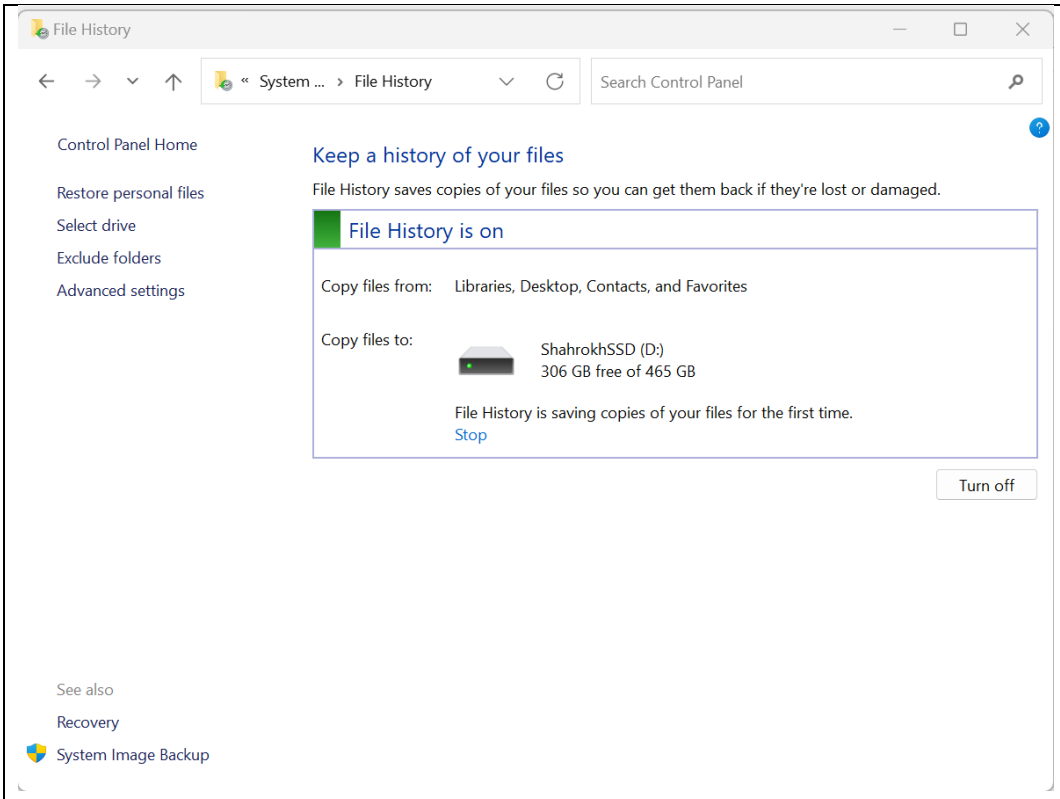

WindowsServer2022 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
wbadmin - [Windows Server Backup (Local)\Local Backup]
File Action View Help
Local Backup
Recovery Wizard
Confirmation
Getting Started
Select Backup Date
Select Recovery Type
Select Items to Recover
Specify Recovery Options
Confirmation
Recovery Progress
From backup: 28/11/2022 11:07 AM
Recovery items:
C:\Security_ShahrokhTahmooreszaeh
Recovery destination: Original location
Recovery option: Create copies of recovered files
Security settings: Recover
< Previous
Next >
Recover
Cancel
Actions
Local Backup
Backup Schedule...
Backup Once...
Recover...
Configure Performance Settings...
View
Help
Status
Last Backup
Status: Successful
Time: 28/11/2022 11:07 AM
View details
Type here to search
11:14 AM
28/11/2022

WindowsServer2022 [Running] - Oracle VM VirtualBox
File Machine View Input Devices Help
wbadmin - [Windows Server Backup (Local)\Local Backup]
File Action View Help
Local Backup
Recovery Wizard
Recovery Progress
Getting Started
Select Backup Date
Select Recovery Type
Select Items to Recover
Specify Recovery Options
Confirmation
Recovery Progress
File recovery progress:
Status: Completed.
Recovery details:
Items
Item
Destination
Status
Data transferred
C:\Security_...
C:\
Completed.
1 KB of 1 KB
To close the wizard, click Close — the recovery operation will continue to run in the background. To view the progress of this operation, open the backup in progress message from the Windows Server Backup console.
< Previous
Next >
Close
Cancel
Actions
Local Backup
Backup Schedule...
Backup Once...
Recover...
Configure Performance Settings...
View
Help
Status
Last Backup
Status: Successful
Time: 28/11/2022 11:07 AM
View details
Type here to search
11:15 AM
28/11/2022

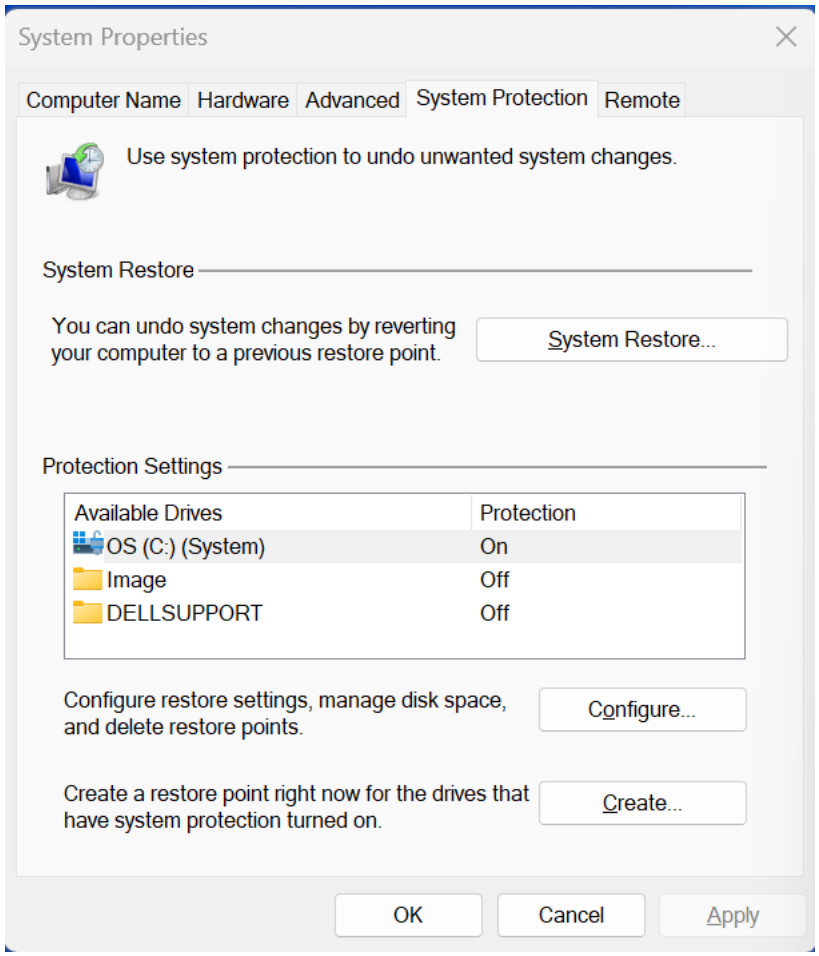


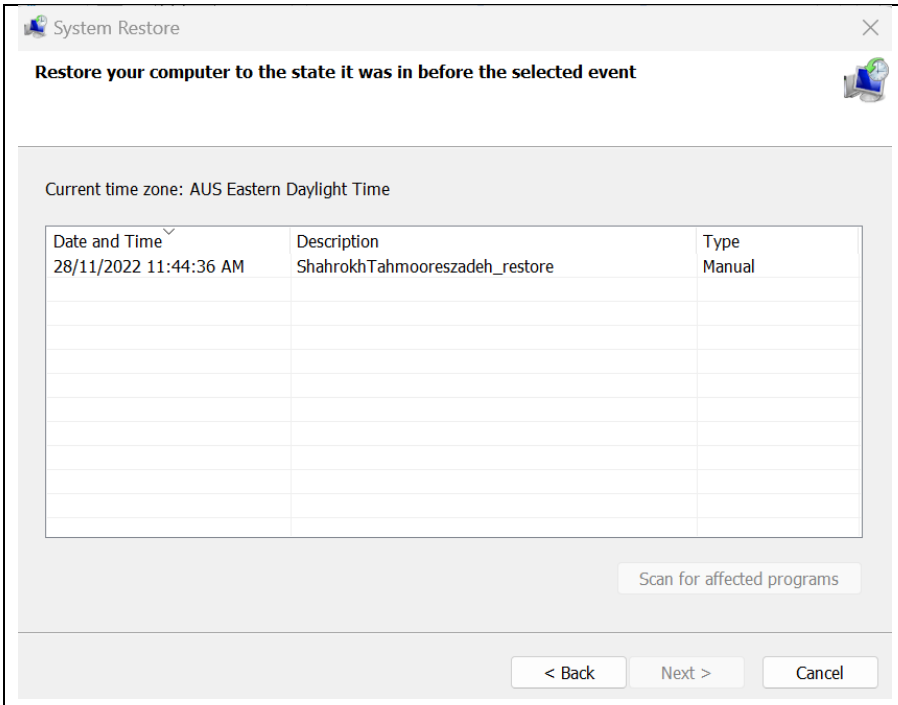


c. Screenshot/s showing the implementation of “Windows File History”

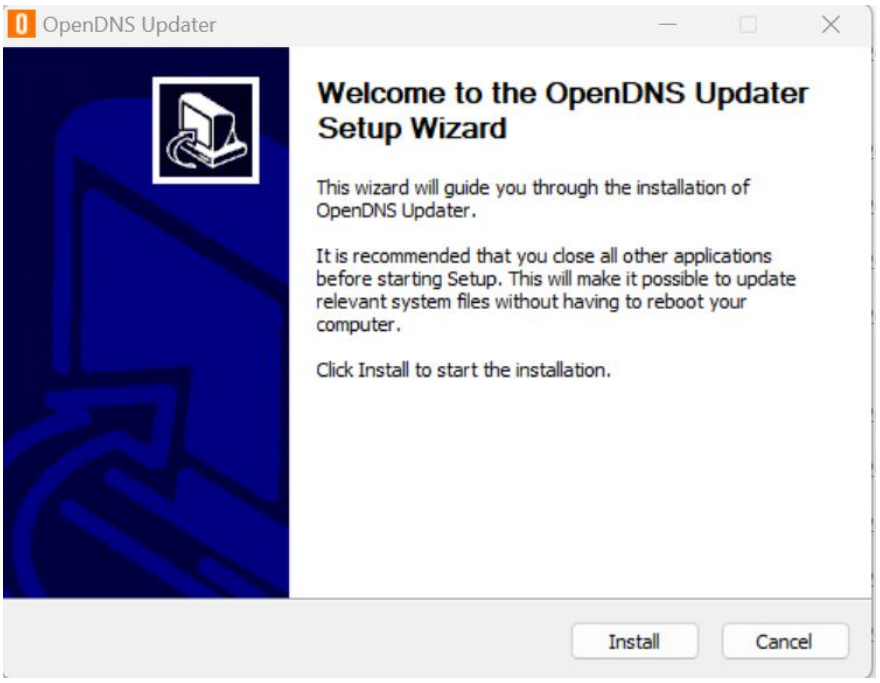


d. Screenshot/s showing a system rollback procedure.

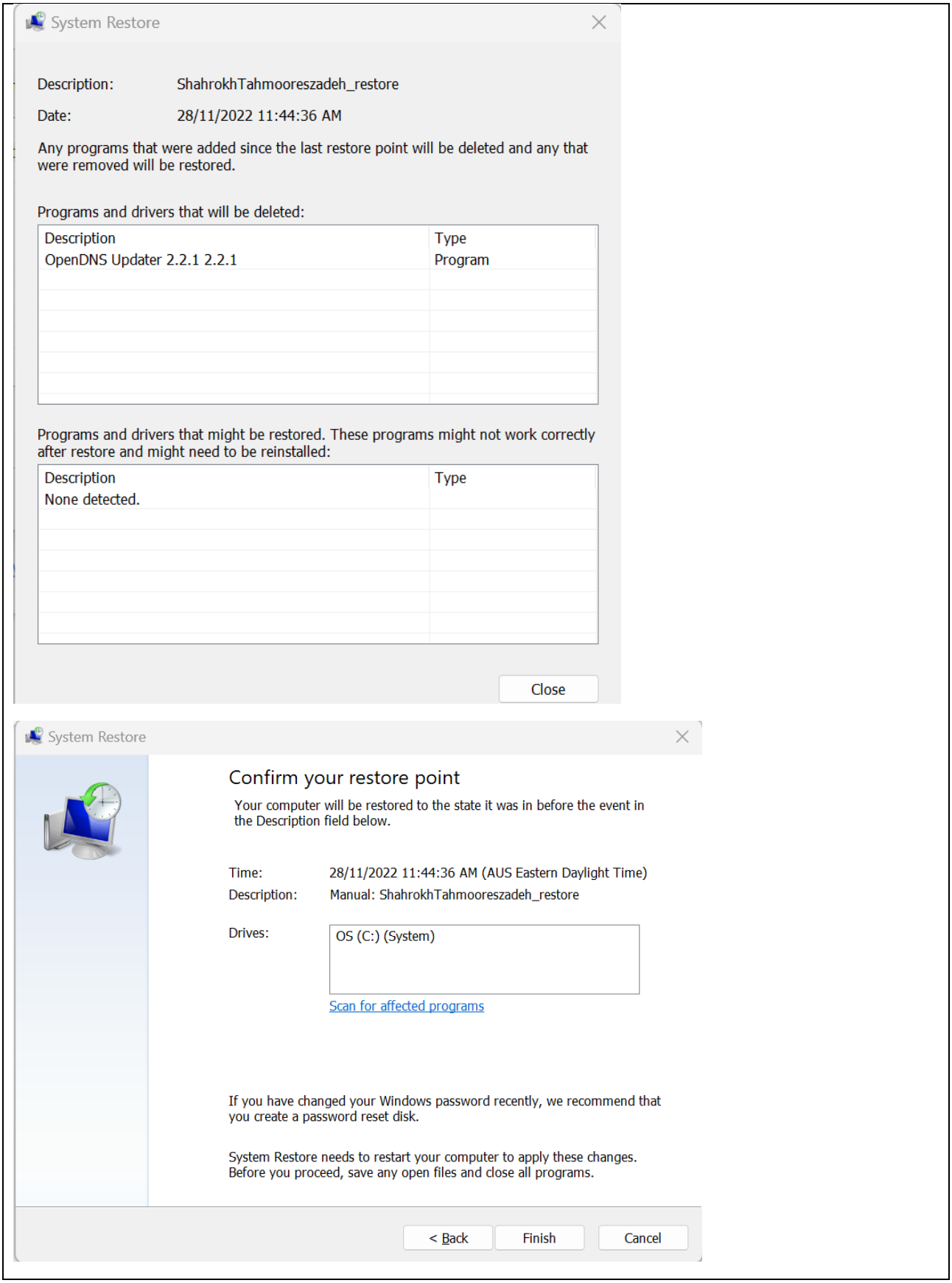




Installing OpenDNS Updater after creating a restore point



Restoring system files and settings


System Restore
Description: ShahrokhTahmooreszadeh_restore
Date: 28/11/2022 11:44:36 AM
Any programs that were added since the last restore point will be deleted and any that were removed will be restored.
Programs and drivers that will be deleted:
Description
Type
OpenDNS Updater 2.2.1 2.2.1
Program
Programs and drivers that might be restored. These programs might not work correctly after restore and might need to be reinstalled:
Description
Type
None detected.
Close
System Restore
Confirm your restore point
Your computer will be restored to the state it was in before the event in the Description field below.
Time: 28/11/2022 11:44:36 AM (AUS Eastern Daylight Time)
Description: Manual: ShahrokhTahmooreszadeh_restore
Drives: OS (C:) (System)
Scan for affected programs
If you have changed your Windows password recently, we recommend that you create a password reset disk.
System Restore needs to restart your computer to apply these changes. Before you proceed, save any open files and close all programs.
< Back
Finish
Cancel

5. Analysis of test results and recommendations

5.1 Network security risks identified during the testing process

Network security risks identified	Impact of risk to security of the business and network	Recommended changes to mitigate the risks
Malware gaining access to the network through the internet	Infecting the PCs	Blocking all connections to application that are not on the list of allowed application
Unauthorised access to the network by cyber attackers	Gaining access to the corporate client data	Setting of rules to spot and prevent cyberattacks