Microsoft Windows Defender & Firewall

**LAB #1:** Access and review Windows Security Virus & threat protection in a virtual environment. Run scans for threats.

1. Navigate to ‘Virus & threat protection’ Windows Security settings. Check for updates, then rua Quick scan for threats.A screenshot of a computer

Description automatically generated

A screenshot of a computer error

Description automatically generated

A screen shot of a computer

Description automatically generated

2. Review Threat history to review results of last scan. Confirm there are no threats in Last scan, Quarantined threats, or Allowed threats sections.

A screenshot of a computer screen

Description automatically generated

3. Run a custom scan that only scans files in Downloads folder.

A screenshot of a computer screen

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer screen

Description automatically generated

**LAB #2:** Configure firewall rules using the Windows Defender firewall in a virtual environment.

1. Access Firewall & network protection settings in Windows Security settings.

A screenshot of a computer

Description automatically generated

2. Confirm Windows Defender Firewall is on for the domain network and the checkbox for blocking incoming connections is unchecked.

A screen shot of a computer

Description automatically generated

3. Confirm the same for the private network, repeat for the public network.

A screenshot of a computer

Description automatically generated

4. In ‘Allow app through firewall’ setting, configure Firefox to communicate on the public network.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

5. For inbound rule ‘Key Management Service (TCP-In)’, deselect allowing public communication.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

6. Create ‘Key Management Service (TCP-In)’ inbound rule that blocks communication with the public network. To do this copy the other ‘Key Management Service (TCP-In)’ rule and configure it. Finally enable both inbound rules.

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer

Description automatically generated

A screenshot of a computer program

Description automatically generated  
A screenshot of a computer

Description automatically generated