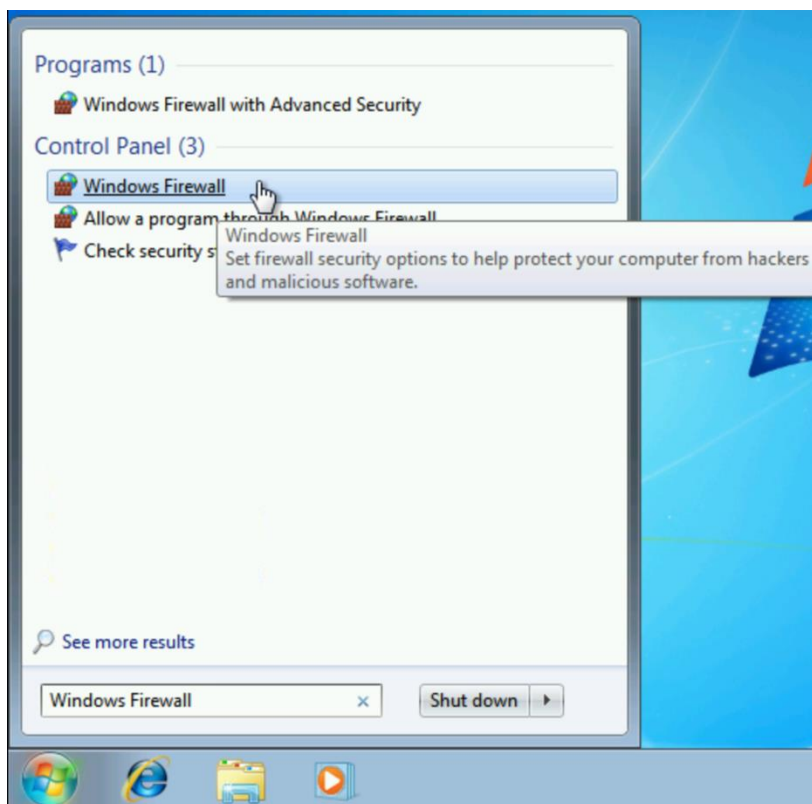


TPT Online Week 3 Lab 6

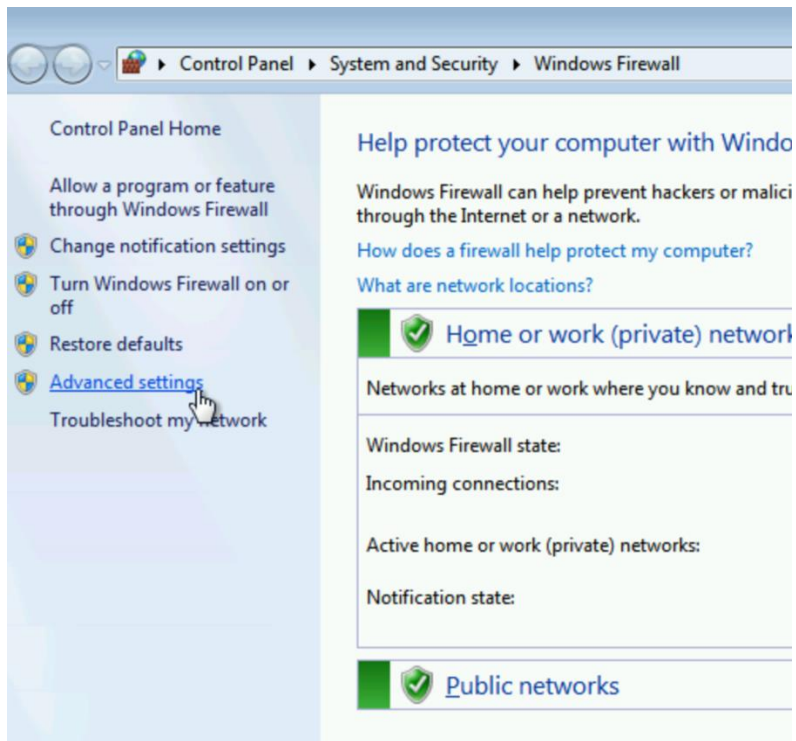
Remediation Scanning End of Life (EOL) Operating System – Windows 7

1. Obtain the IP address of your Windows 7 VM
2. Login into your Kali VM
3. Open your browser and sign into your Nessus web console
4. Create a new scan and set the target IP address to your Windows 7 VM
5. After the scan finishes record the number for vulnerabilities found
6. Login into your Windows 7 VM and turn on the Windows Firewall

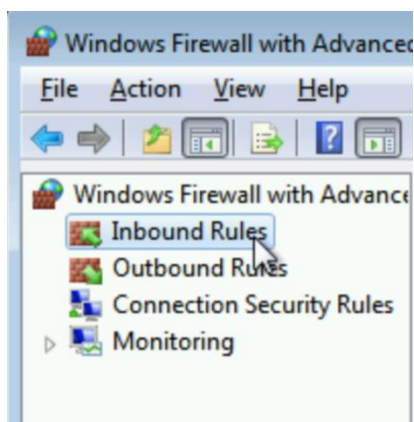


7. Run the scan again against the Windows 7 VM from your Kali VM
8. Any difference in the scan and the scan results?
9. If so explain

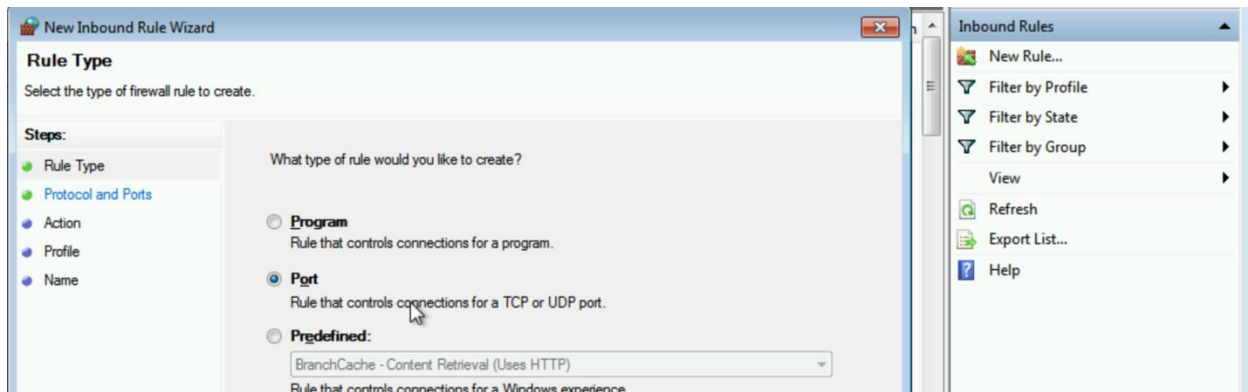
10. Focus your attention on the detected vulnerabilities on server message block (SMB)
11. Log back into the Windows 7 VM and create a custom firewall rule
12. Go to Control Panel > System Security > Windows Firewall > Advanced settings



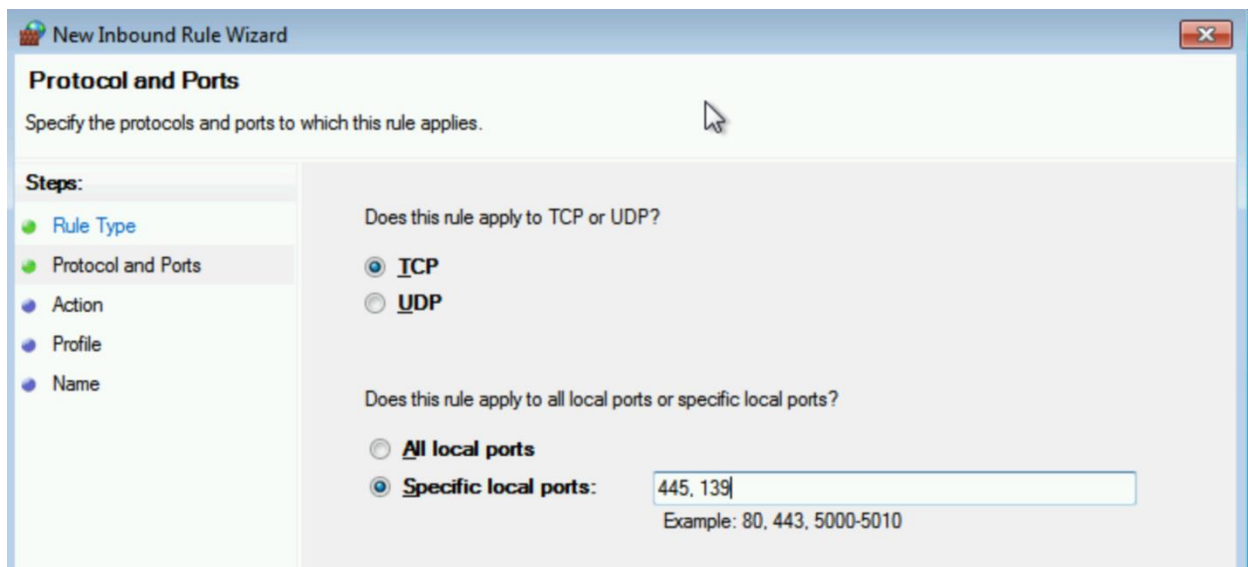
13. Click on Inbound rules



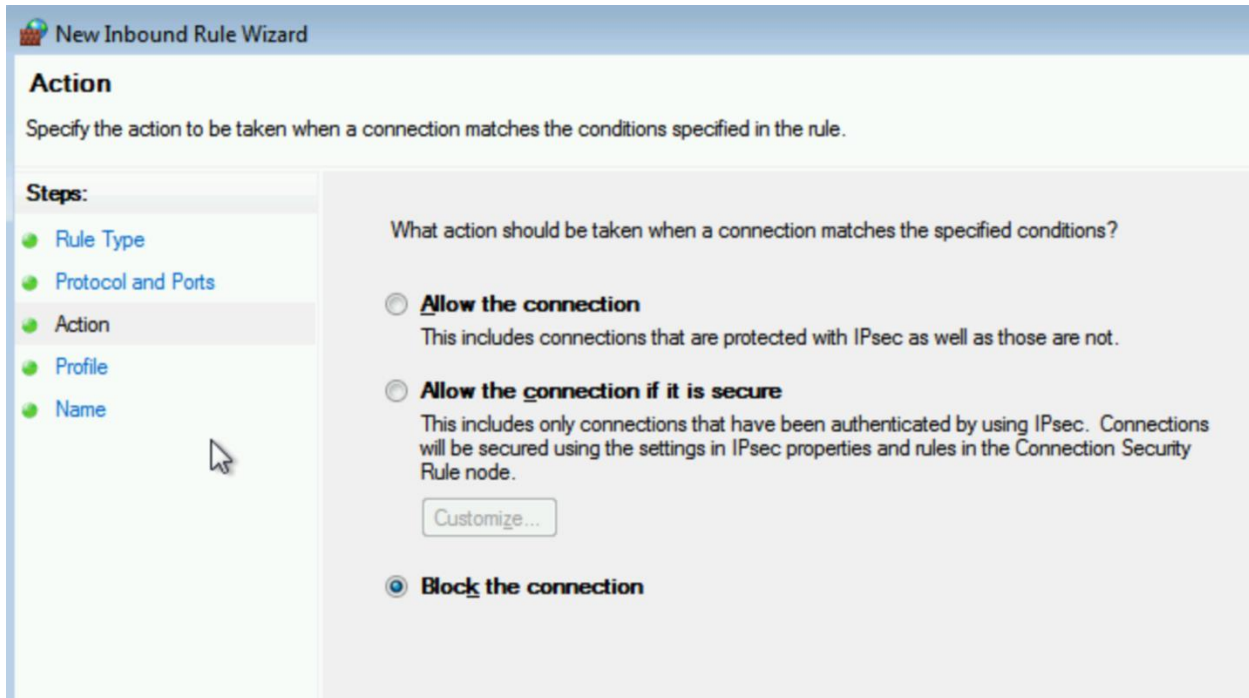
14. Create a new rule and select port



15. Choose TCP and type in port 445, 139



16. In the inbound rule wizard select “Block Connections”



The screenshot shows the 'New Inbound Rule Wizard' window, specifically the 'Action' step. The left sidebar lists the steps: Rule Type, Protocol and Ports, Action (selected), Profile, and Name. The main area is titled 'Action' and contains the instruction 'Specify the action to be taken when a connection matches the conditions specified in the rule.' Below this, a question asks 'What action should be taken when a connection matches the specified conditions?'. There are three radio button options: 'Allow the connection' (unselected), 'Allow the connection if it is secure' (unselected), and 'Block the connection' (selected). Each option has a descriptive text block. A 'Customize...' button is located below the 'Allow the connection if it is secure' option.

New Inbound Rule Wizard

Action

Specify the action to be taken when a connection matches the conditions specified in the rule.

Steps:

- Rule Type
- Protocol and Ports
- Action**
- Profile
- Name

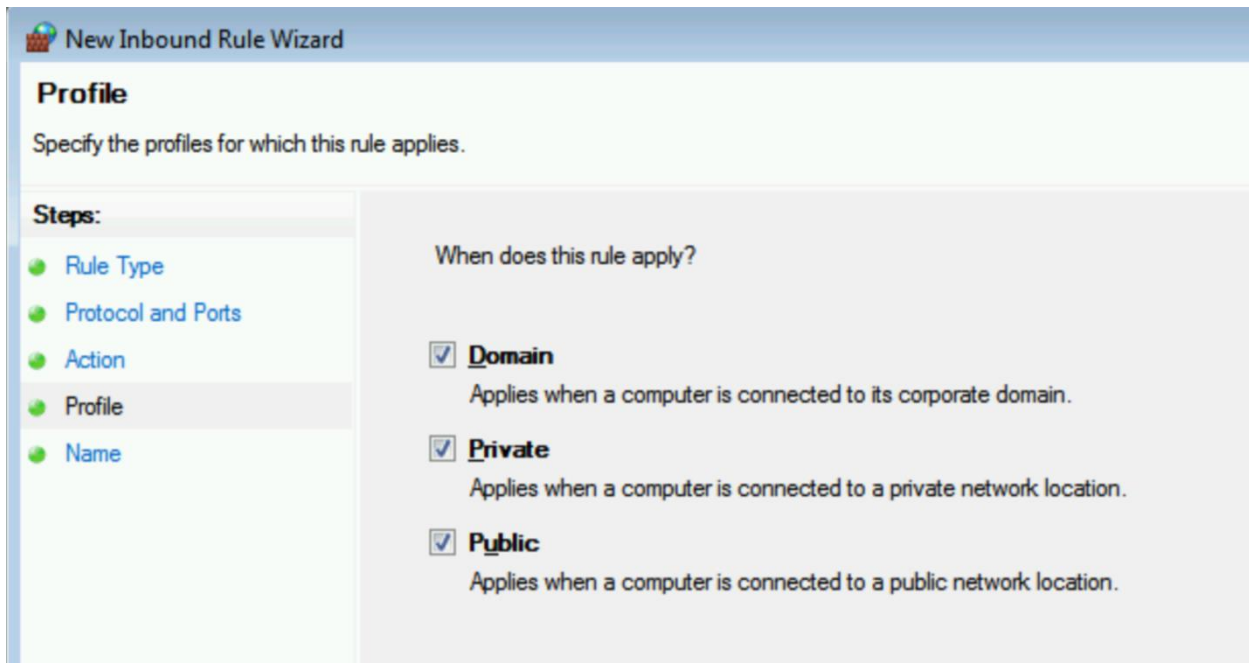
What action should be taken when a connection matches the specified conditions?

☐ **Allow the connection**
This includes connections that are protected with IPsec as well as those are not.

☐ **Allow the connection if it is secure**
This includes only connections that have been authenticated by using IPsec. Connections will be secured using the settings in IPsec properties and rules in the Connection Security Rule node.

☒ **Block the connection**

17. In the profile section select all select Domain, Private and Public



The screenshot shows the 'New Inbound Rule Wizard' window, specifically the 'Profile' step. The left sidebar lists the steps: Rule Type, Protocol and Ports, Action, Profile (selected), and Name. The main area is titled 'Profile' and contains the instruction 'Specify the profiles for which this rule applies.' Below this, a question asks 'When does this rule apply?'. There are three checked checkbox options: 'Domain', 'Private', and 'Public'. Each option has a descriptive text block.

New Inbound Rule Wizard

Profile

Specify the profiles for which this rule applies.

Steps:

- Rule Type
- Protocol and Ports
- Action
- Profile**
- Name

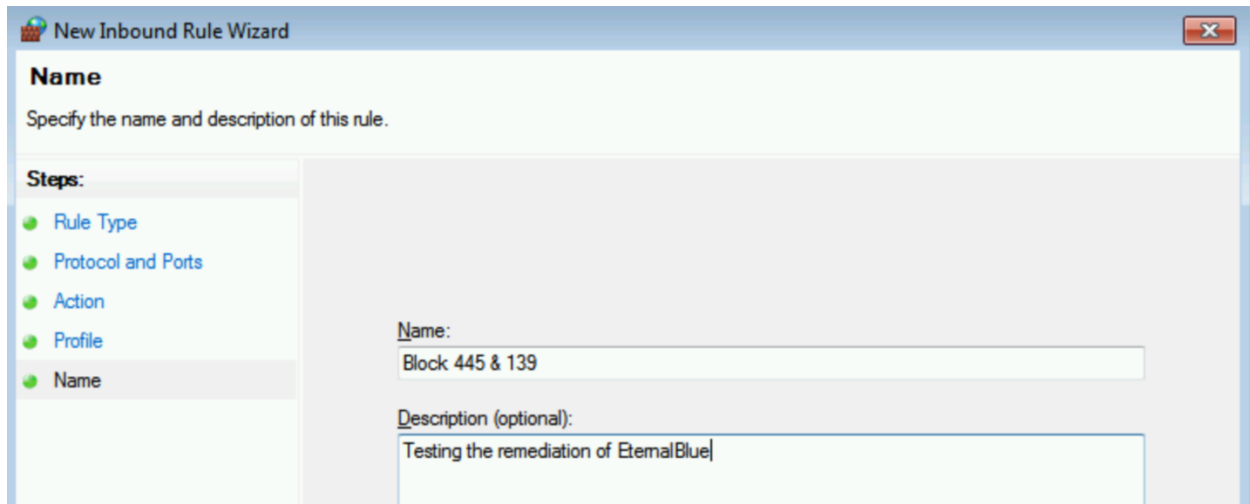
When does this rule apply?

☒ **Domain**
Applies when a computer is connected to its corporate domain.

☒ **Private**
Applies when a computer is connected to a private network location.

☒ **Public**
Applies when a computer is connected to a public network location.

18. Provide a descriptive name for your custom rule and save the rule



19. Re-run the scan from the Kali VM

20. Are the SMB vulnerabilities still present after the scan?

21. What other ports could you block to remediate the vulnerability findings from the Nessus scan?

- a. Hint: Look at the critical vulnerabilities to identify the port Nessus scanned to find the vulnerability.
- b. If you identified a port, repeat steps 12-18 to create a firewall rule on the Windows 7 VM and re-run a scan to validate the additional vulnerabilities found on that identified port are no longer present.

22. Provide your answers in a Word document and save it with first name_last_name_Threat Protection & Testing_Week 4_Lab6.

23. Upload to the FSO Lab assignment module.