Jessica Sullivan

Netlab+ Lab 10: Network Security – Firewalls

1. *Describe a host-based firewall.*

*Answer: A host-based firewall is designed to protect an individual computer to prevent malicious traffic to getting on its system or network. The host-based firewall is software on the computer.*

1. *Describe a network-based firewall.*

Answer: A network based firewall is located between the internal and external networks. It inspects traffic between networks rather than protecting individual computers.

1. *Which type of firewall is Windows Firewall?*

Answer: Windows Firewall is a host-based firewall intended to secure individual computers by filtering network traffic.

1. *Explain the Notification state in Windows Firewall.*

Answer: The notification state is an option that details what notifications have been configured for a Windows Firewall. Such a notification would be for when something gets blocked.

1. *Discuss why network profiles are important.*

Answer: Windows Firewall associates a profile to a network location type allowing for specialization of firewall rules depending on the connection type. Domain, Private, and Public have different security risks and therefore need specialized security settings.

1. *Describe the three types of profiles found in the Windows Firewall.*

Answer:

* Domain: Domain profiles are applied to the network adapter when a computer is connected to a network and can contact the domain through a domain controller.
* Private: Private profiles are applied to the network adapter when the computer is connected to a network behind a network firewall or some type of security device. These are more restrictive than domain profiles.
* Public: applied to a network adapter when it is connected to a public network, this is even more restrictive because the lack of security control.

1. *Explain and give an example of network locations.*

Answer: Domains are generally found at work, private networks are usually at home, and something like the Wi-Fi at starbucks would be considered a public network. Public networks have a lot more foot traffic and so there’s more likely to be someone looking for vulnerabilities than at home or work.

1. *In Windows Firewall, what do the Home/Work (Private) and Public columns indicate?*

Answer: The different columns indicate what kind of network the computer must be associated with in order to unblock these programs. The need for more or less restriction changes based on location.

1. *Define the term: firewall rule (exception).*

Answer: Firewall rules (exceptions) are created to allow and block specific traffic.

1. *Explain why it is a risk to allow programs and add exceptions through the firewall.*

Answer: Adding firewall exceptions are poking holes in the firewall that are meant to protect your computer. The more exceptions available the more vulnerable the machine is to exploitation.

1. *Explain why it isn’t necessary to create an inbound rule on the Windows 2k8 R2 Internal 1 machine so that it can receive the response (ICMP echo reply) from the Windows 2k8 R2 Internal 2 machine.*

Answer: The reply is not an unsolicited response. Part of the ping operation is to receive some feedback. Therefore there does not need to be special handling to receive responses.

1. *Identify the four basic types of firewall rules.*

Answer: The four basic types of firewall rules are: inbound, outbound, unilateral in/outbound and bidirectional in/outbound rules.

1. *Compare the ufw status verbose command output with Windows Firewall with the Advanced Security Windows Firewall Properties you investigated in an earlier lab. Describe the major similarities that you observe.*

Answer: After adding the telnet rule, the similarities are more apparent. While both Windows Firewall and ufw seem to show the same information: what program is blocked and what bound traffic is blocked. However, the Windows firewall is more intuitive and specifies different profiles whereas the ufw seems to only work in global terms.

1. *Explain the advantages and disadvantages of having the firewall disabled at start up in the Linux operating system.*

Answer: A benefit to having the firewall disabled at start up is that inexperienced people using the machine won’t accidentally poorly configure the firewall in a way that impacts their use. Most Linux OS’s automatically disable some of the more vulnerable ports. However the disadvantages are that your computer is more at risk for attack at start up.

1. *Create and document two firewall rules that you think would be important to include if all outbound traffic is being denied by the firewall rules. Explain your decision.*

Answer: The first firewall rule that we want to include is to make sure that all inbound traffic is blocked except LAN access. Next we want to allow outbound traffic to the LAN. These will result in greater security accessing the internet.