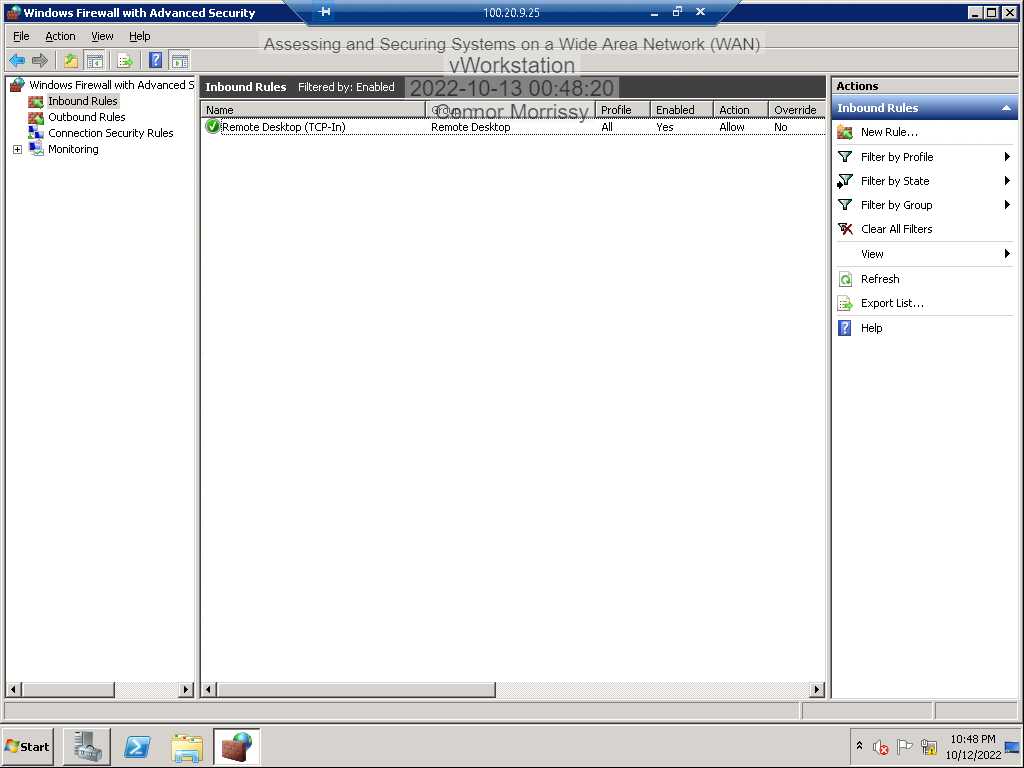
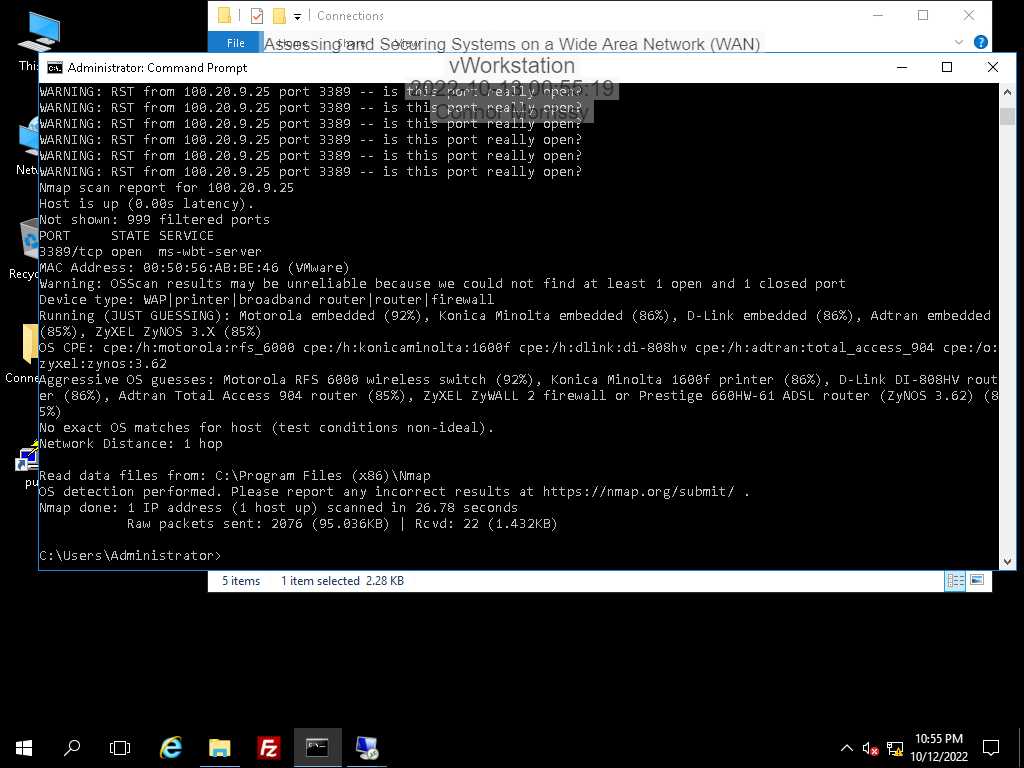
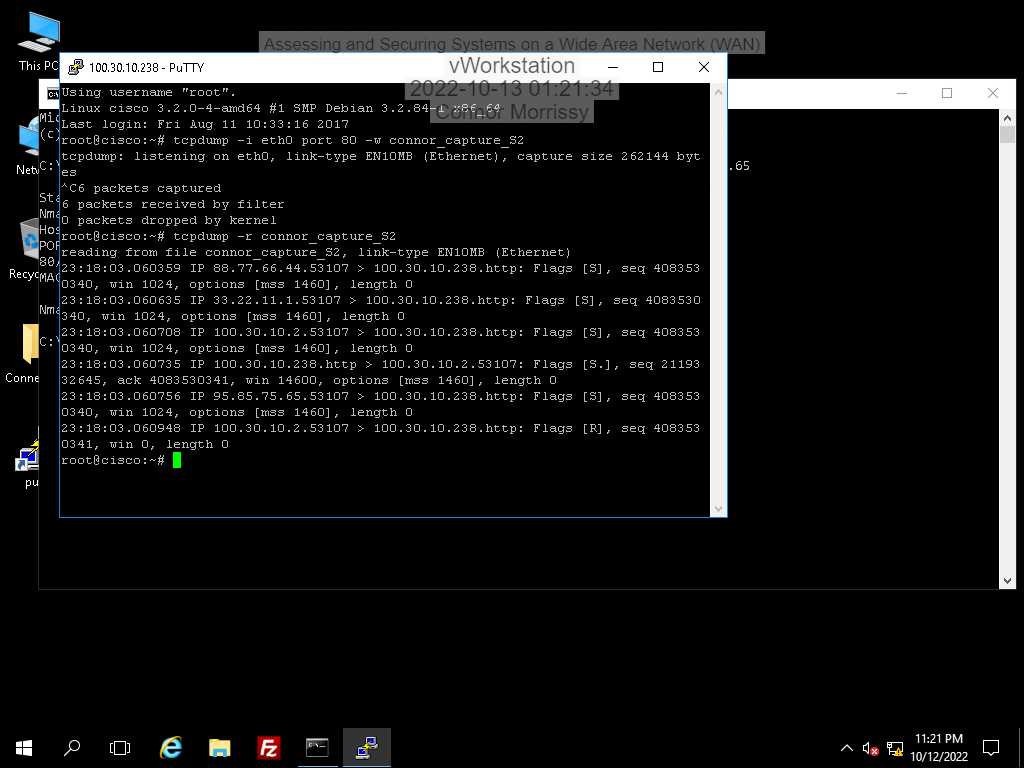


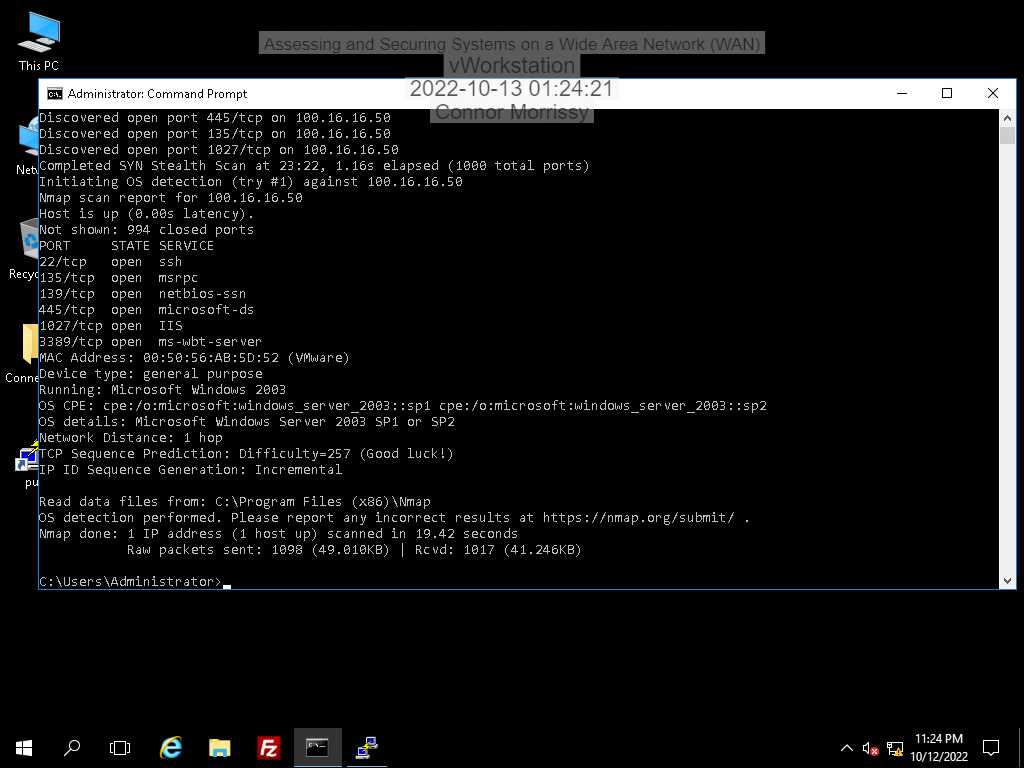
After making an exception for port 3389 for RDP connection in the firewall and turning it on, device 100.16.16.50 has blocked all open ports except for port 3389, as seen in the nmap scan.

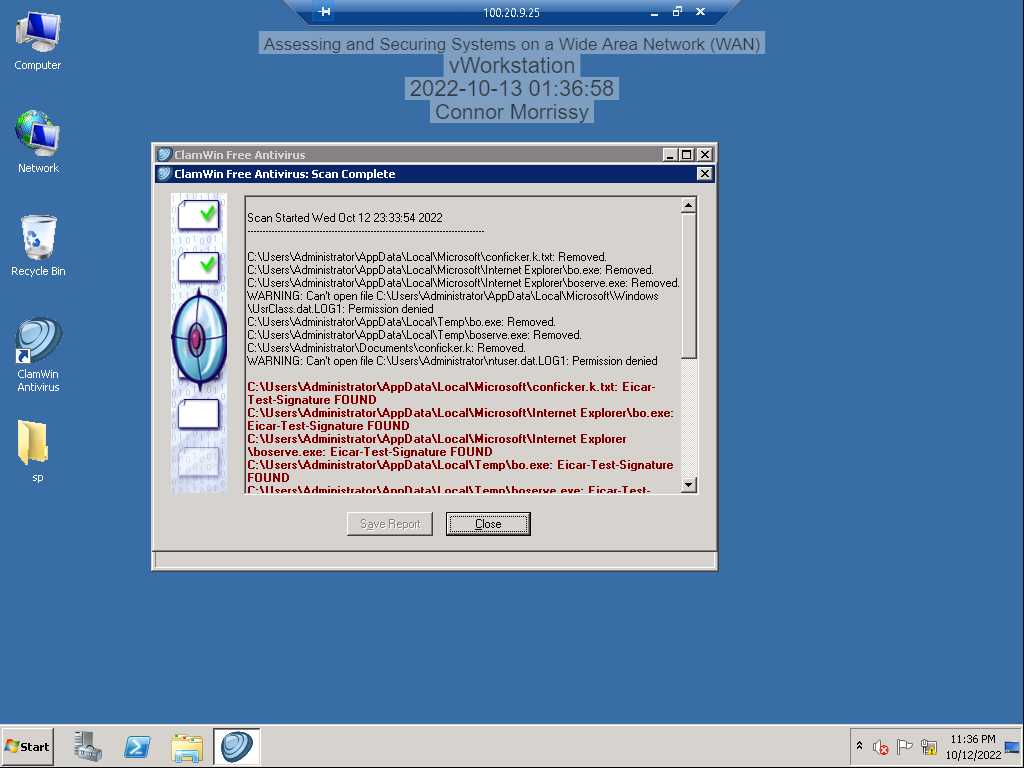


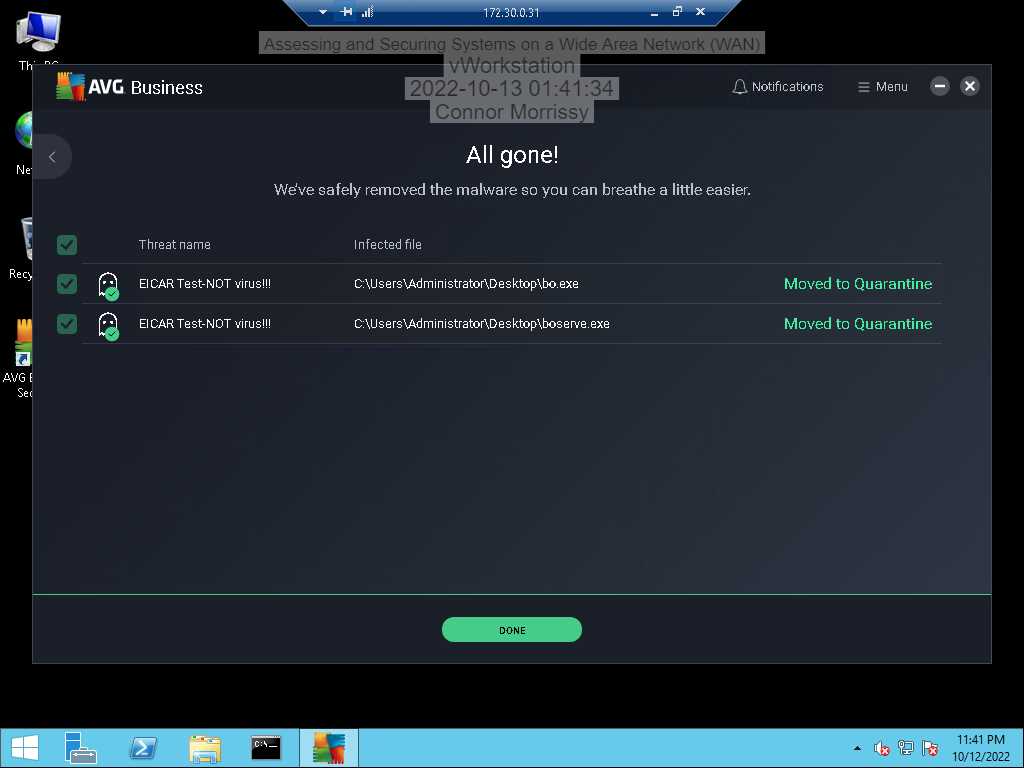


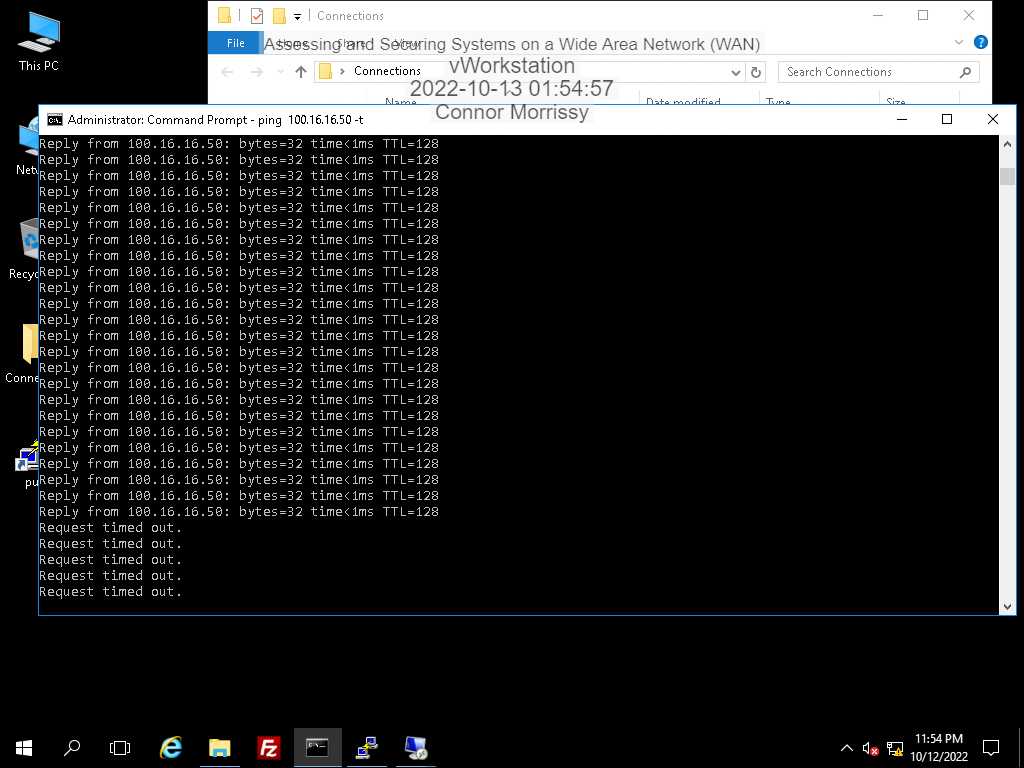
I went into the firewall settings on the Windows 2008 machine and disabled all ports in the firewall except for port 3389, which hardened the security.

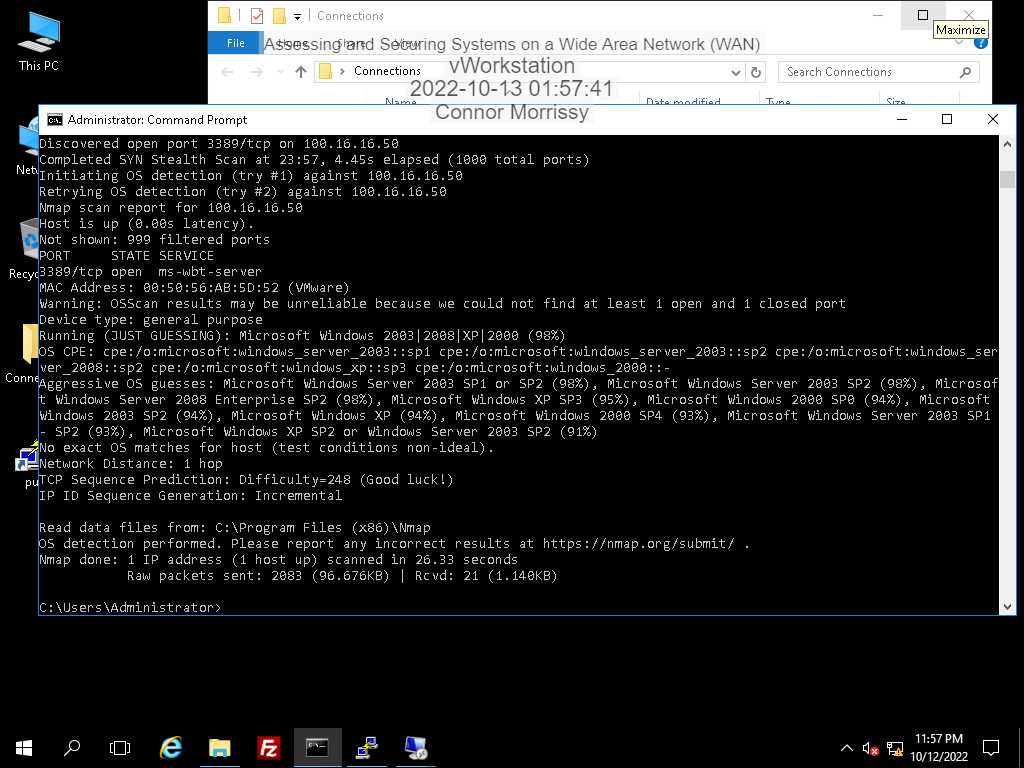




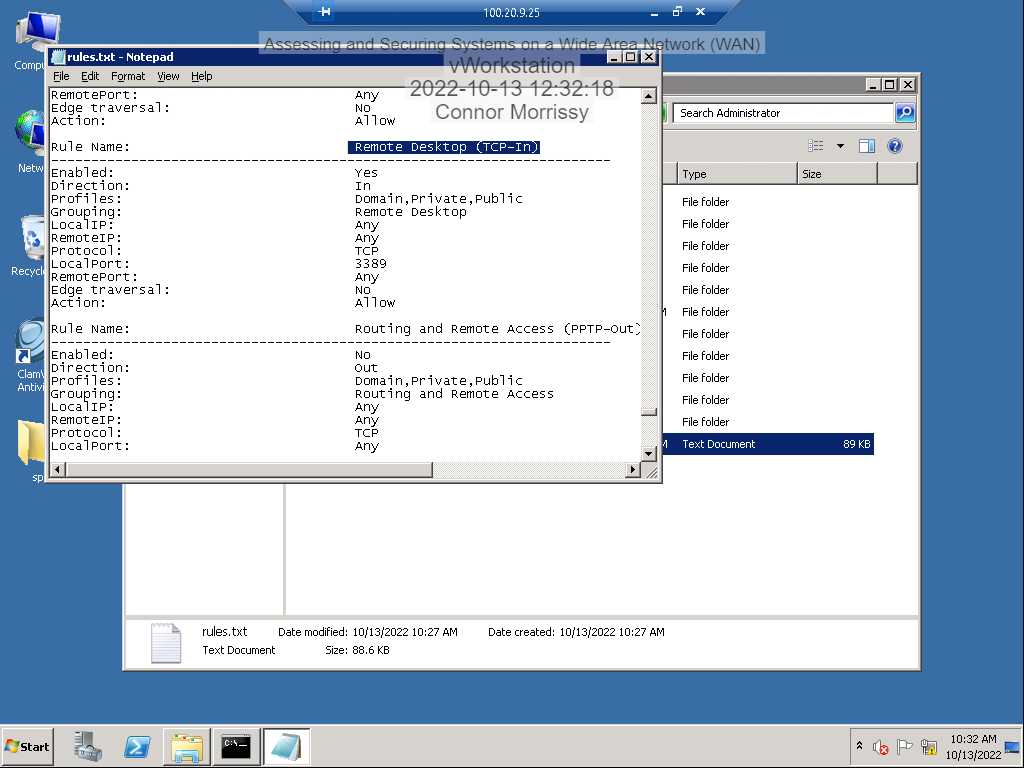


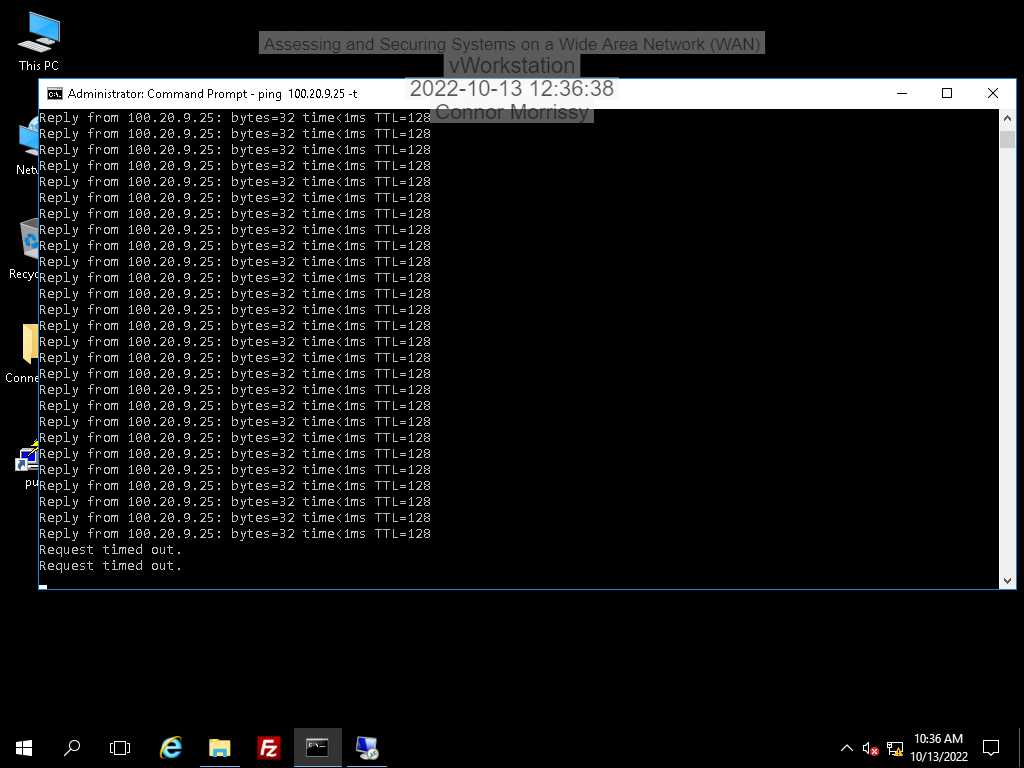


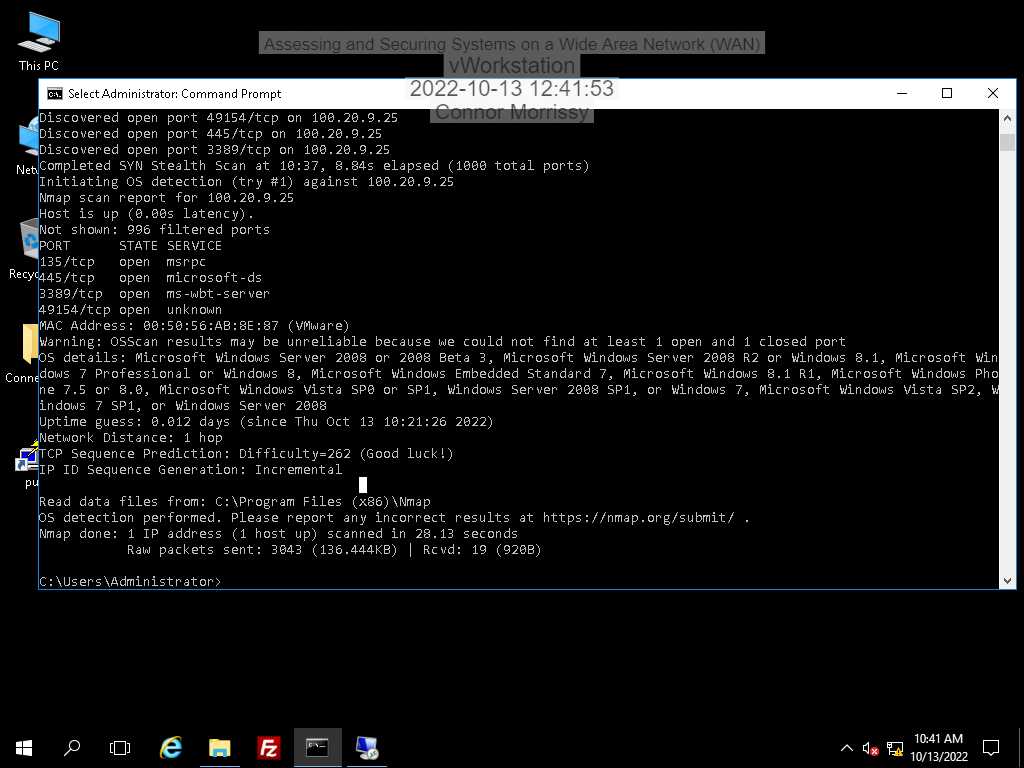




I manually configured the firewall on the TargetVulnerable01 machine to block all open ports and to allow RDP remote connections, which hardened the security on this device.







The firewall was turned on and ICMPv4 messages were blocked in the firewall, which prohibits pings and scans of the network, which hardens the device’s security.

**Section 3:**

Part 1:

The name of the Back Orifice exploit originates from the Windows NT software called Back Office. It’s still dangerous because it can provide an unauthorized person administrator access, allowing them to do almost anything they want.  
  
Part 2:

2003: netsh firewall add portopening UDP 445 samba enable  
2008: netsh advfirewall firewall set rule group=”File and Printer Sharing” new enable=yes  
  
  
Part 3:

1. 