**Q9**

**Windows Network Configuration**

Take the following precautions to protect a Windows Server machine from network attacks:

Place the machine behind the firewall—production Windows Server instances should always run in a protected network segment.

Redundant DNS—configure two or more DNS servers and verify name resolution using nslookup.

Verify DNS records—ensure the server has an A record and PTR record for reverse DNS lookups.

Disable network services—any service the server is not actually using, like IPv6, should be disabled to reduce the attack surface.

**Network Time Protocol (NTP) Configuration**

Windows login and other functions that leverage kerberos security rely on accurate NTP times. Even a small time difference can break functionality. To avoid service disruption, make sure that:

Servers within domains automatically sync time with the domain controller

Standalone servers sync with an external time source

Domain controllers sync with a time server on an ongoing basis

**For Linux**

<https://www.pluralsight.com/blog/it-ops/linux-hardening-secure-server-checklist>