Brian Johnson

3/28/2023

**Nessus Scan Assignment (Core)**

* Ran a Nessus scan on my router and it discovered several vulnerabilities, 1 of a medium severity.
* That severity is a “SMB (Server Message Block) Signing Not Required”.
* It means computers on the network are not checking id data that’s coming in is from a legitimate source or if it has been tampered with.
* Man In the Middle Attacks. This allows attackers to intercept, modify, or inject malicious data between computers leading to access or data left.
* Like sending mail without a seal, so anyone can read or modify it without anyone knowing.

**Mitigating**

* Update your systems: Make sure all your devices and operating systems are up-to-date with the latest security patches.
* Enable SMB Signing: For Windows-based systems, you can enable SMB Signing through Group Policy or Local Security Policy.
* Restrict access: Limit access to shared resources on your network by implementing strong access controls, such as password policies, user authentication, and network segmentation.
* Use encryption: Whenever possible, use encryption to protect data in transit. This can be achieved through technologies like IPsec (Internet Protocol Security) or VPN (Virtual Private Network) connections.

A screenshot of a computer

Description automatically generated

