

The Arkansas Cyber Defense Center

Man in the Middle Attack

In this type of attack, the perpetrator positions themself in a conversation between a user and an application in order to impersonate one of the parties or eavesdrop to gain information.

What do threat actors want?

The goal of this attack is to steal information (login credentials, credit card numbers, etc.). Additionally, it can be used to gain access to a secured network perimeter.

Tactics of this kind of attack:

<u>IP Spoofing:</u> Altering packet headers to disguise an IP address <u>DNS spoofing:</u> Altering a website's address record in order to catch the websites incoming traffic

<u>ARP spoofing:</u> Linking the attacker's MAC address to the IP address of a legitimate user on a LAN to get access to the user's traffic.

Prevention:

- Avoid using WiFi that isn't password protected.
- Heed the warnings of browser notifications saying the website is unsecure.
- Log out of applications that aren't in use.
- Avoid public networks.



Information provided by Forge Institute or any of its employees, contractors, or advisors does not constitute expert or technical advice for any particular matter. Due to the complex nature of cyber, individuals or companies should seek advice from their insurer, attorney or managed service provider. Nothing contained herein should be construed as consultative advice. Forge Institute bears no liability arising in connection with the information it provides. Use of Forge Institute information constitutes agreement to the legal Terms & Conditions & Privacy Policy located at www.forge.institute/terms. The Forge Institute ACDC is funded, in part, through a Cooperative Agreement with the U.S. Small Business Administration. All opinions, and/or recommendations expressed herein are those of the authors(s) and do not necessarily reflect the views of the SBA. REPORT A CYBER INCIDENT:

forge.institute/acdc 501-239-9599

