AUSJOURNAL
ISSN: 2200-1883

Published by SISTMR Australia
ISSN: 2200-1883 | www.ausjournal.com

VOLUME	ISSUE	YEAR
Vol. 1	Issue 1	2026
PAGES	**DOI**	**ARTICLE TYPE**
1 – 8	[10.xxxx/ausjournal.v1i1.001]	Research Article

ARP Poisoning and Man-in-the-Middle (MITM) Attacks

Dr. Pritam Gajkumar Shah

SISTMR Australia, Sydney, Australia

Corresponding author: *[wsnpgs@gmail.com]*

Received: [2nd January 2026] | Accepted: [22nd January 2026] | Published: [22nd January 2026]

ABSTRACT

Address Resolution Protocol (ARP) poisoning is a common network-based attack technique that enables Man-in-the-Middle (MITM) attacks within local area networks. By exploiting the stateless nature of ARP, an attacker can intercept, monitor, and potentially alter network information between communicating hosts. This paper provides an empirical overview of ARP poisoning and MITM attacks, discusses their impact on network security, illustrates observations using packet capture screenshots, and outlines practical prevention and mitigation strategies suitable for academic and enterprise environments.

Keywords: ARP poisoning; MITM attack; Wireless security; Network security; Packet analysis

How to cite this article: Shah, P. G. (2026). ARP Poisoning and Man-in-the-Middle (MITM) Attacks. *AusJournal*, 1(1), 1 – 8.

1. INTRODUCTION

Modern computer networks rely on protocols that were originally designed without strong security controls. ARP is one such protocol, responsible for mapping IP addresses to MAC addresses within a local network. Because ARP lacks authentication, it is vulnerable to spoofing and poisoning attacks. Attackers can leverage this weakness to position themselves between two communicating parties, resulting in a Man-in-the-Middle (MITM) scenario [1].

2. BACKGROUND: ARP AND MITM ATTACKS

ARP poisoning occurs when an attacker sends forged ARP replies to victims, associating the attacker's MAC address with the IP address of another host, typically the default gateway. Once poisoned, traffic intended for the legitimate host is redirected through the attacker. In a MITM attack, this allows passive eavesdropping or active manipulation of traffic, including credential interception and session hijacking [2].

3. OBSERVATION METHODOLOGY (HIGH-LEVEL)

To study ARP poisoning and MITM behavior in a controlled laboratory environment, a network analysis tool capable of packet sniffing and protocol dissection was used. Traffic was observed before and after ARP cache manipulation to identify changes in packet flow, host communication paths, and the appearance of sensitive information in captured sessions. No operational steps or exploit instructions are provided in this paper [3].

4. PRACTICAL EVIDENCE

Figure 1 illustrates observed HTTP credential exposure during intercepted traffic, captured in a controlled academic environment to demonstrate the visibility risk posed by unencrypted protocols when ARP poisoning is present.

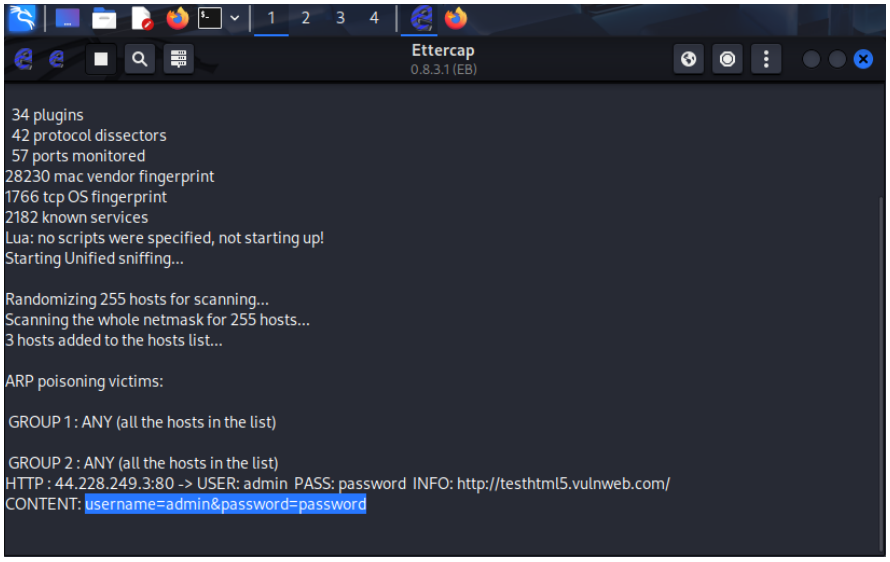

Figure 1. *Observed credential exposure in an intercepted HTTP session within a controlled lab.*

Figure 2 shows a conceptual interface indicating ARP-based MITM activity within the network.

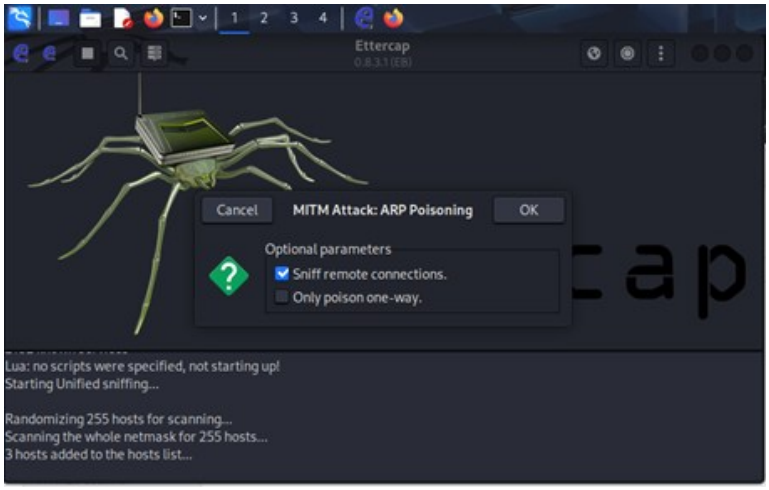

Figure 2. *Conceptual interface indicating ARP-based MITM activity.*

5. SECURITY IMPACT

The impact of ARP poisoning–based MITM attacks includes loss of confidentiality, compromise of authentication credentials, data manipulation, and erosion of trust in network services. In academic labs, such attacks demonstrate protocol weaknesses; in real-world networks, they pose significant operational and compliance risks [4].

6. PREVENTION AND MITIGATION STRATEGIES

Effective mitigation includes the use of Dynamic ARP Inspection (DAI) on managed switches, static ARP entries for critical hosts, network segmentation, encrypted protocols such as HTTPS and TLS, and

continuous monitoring with intrusion detection systems. Security awareness and regular audits further reduce exposure to MITM attacks.

7. CONCLUSION

ARP poisoning remains a relevant threat due to inherent protocol limitations. Understanding its mechanics at a conceptual level enables defenders to design stronger network controls. By combining technical safeguards with monitoring and education, organizations can significantly reduce the risk of MITM attacks.

ACKNOWLEDGEMENTS

[Optional: acknowledge any contributors, reviewers, or institutional support here.]

Funding: This research received no external funding.

Conflict of Interest: The author declares no conflict of interest.

Ethics Statement: All observations were conducted in a controlled laboratory environment for educational and defensive research purposes. No live or third-party networks were targeted.

REFERENCES

[1] Bellovin, S. M. (2003). A look back at "Security Problems in the TCP/IP Protocol Suite." *Computer Security Applications Conference*. https://doi.org/10.1109/CSAC.2003.1254347

[2] Cisco Systems. (2022). *Dynamic ARP inspection*. https://www.cisco.com/

[3] Scapy Project. (2021). *ARP spoofing and packet manipulation*. https://scapy.net/

[4] Stallings, W. (2020). *Network security essentials: Applications and standards* (6th ed.). Pearson.