UJAR TECH SOLUTION

NAME: Rithik varma

INTERN ID: UTS1103

TASK 9

Man-in-the-Middle (MITM) Attack Using Ettercap or MITMf:

Understand how Man-in-the-Middle (MITM) attacks work on a local network by performing ARP spoofing to intercept and monitor traffic between two devices.

PRACTICAL DESCRIPTION

Problem:- *Explore a Linux machine to understand how Man-in-the-Middle (MITM) attacks work by using ARP spoofing to intercept and monitor traffic between two devices on a local network.*

Key Concepts of Man-in-the-Middle:

A Man-in-the-Middle (MITM) attack occurs when an attacker secretly positions themselves between two communicating parties (e.g., a user and a server) and:

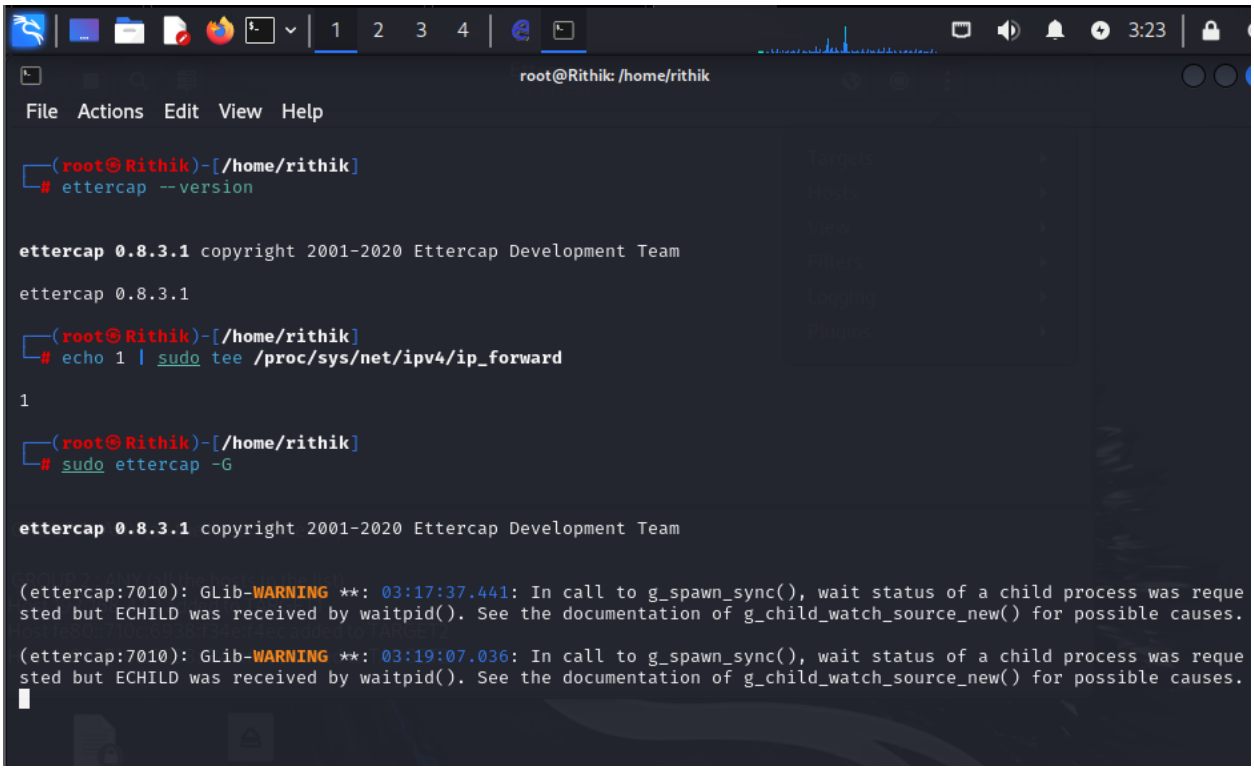
- *Eavesdrops on the communication*
- *Modifies traffic (injects malicious code, redirects sessions)*
- *Steals sensitive data like login credentials, cookies, or session tokens*

Tools Used

- *Ettercap – A popular tool for performing MITM attacks (supports ARP spoofing, sniffing, and traffic manipulation).*
- *MITMf (Man-in-the-Middle Framework) – A more advanced framework that includes modules for credential harvesting, session hijacking, and code injection.*

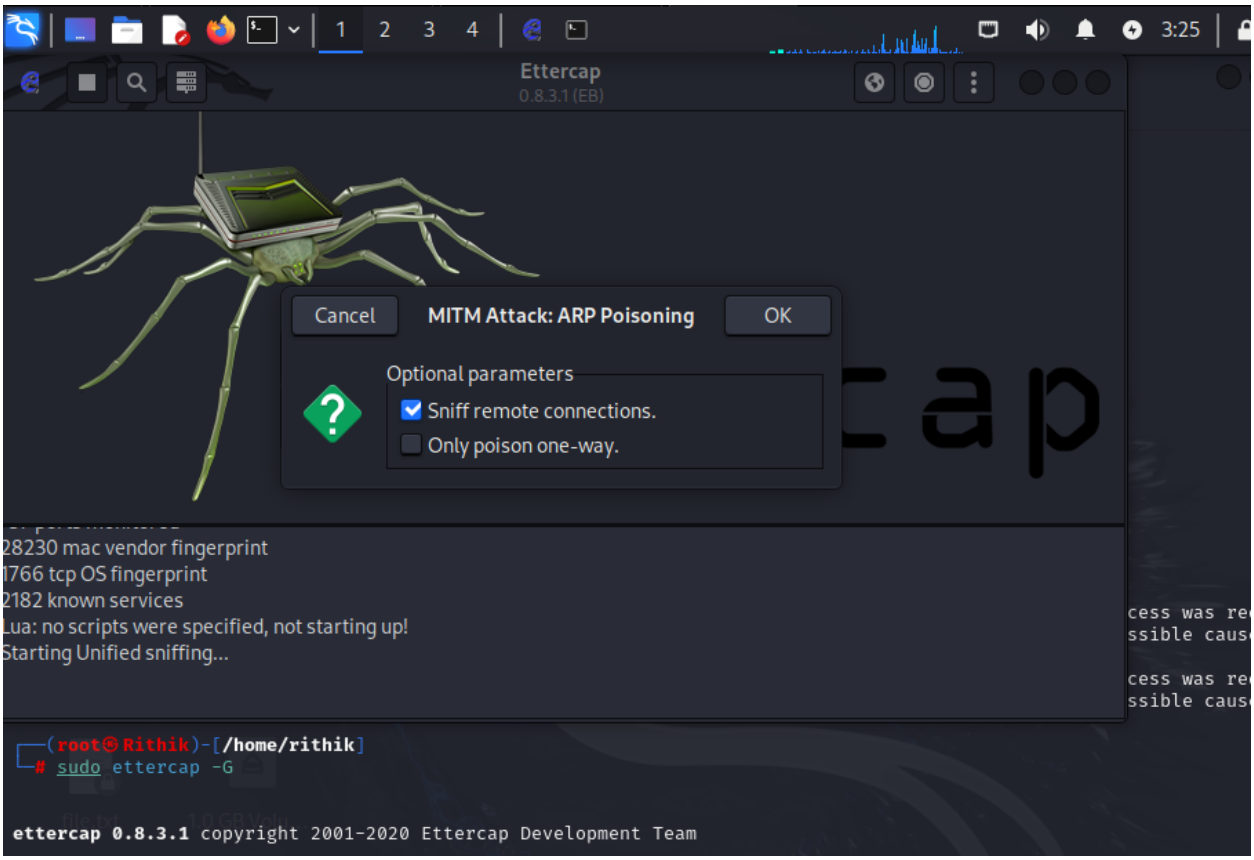
Practical of MITM Attack Using Ettercap Using Kali Linux:-

Installing and running ettercao.

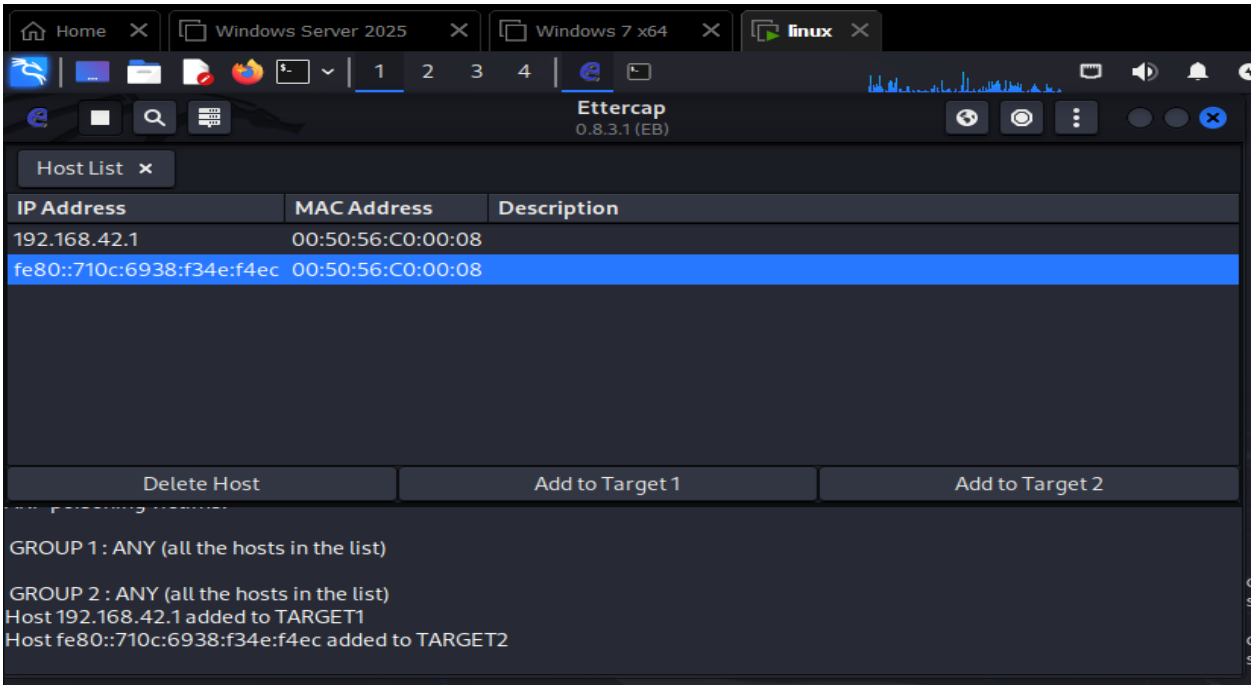


Start Ettercap in Text or GUI Mode

Enable ARP Spoofing

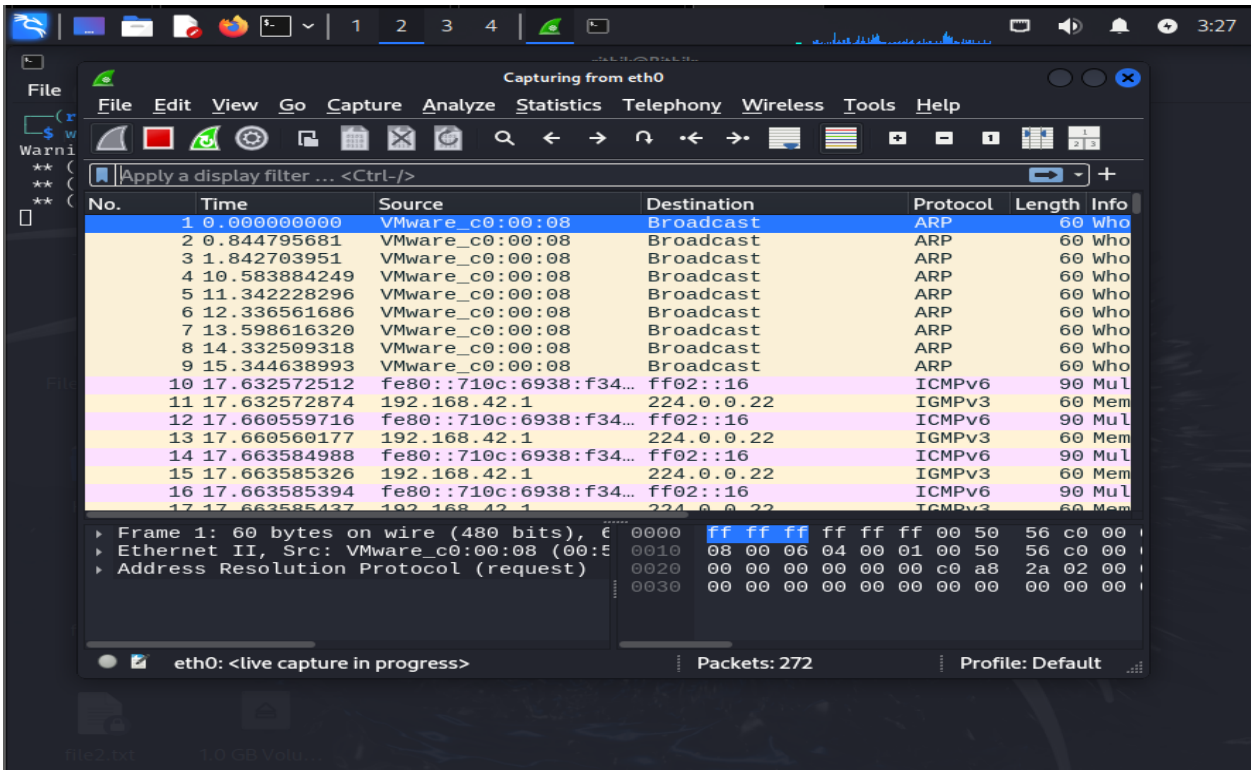


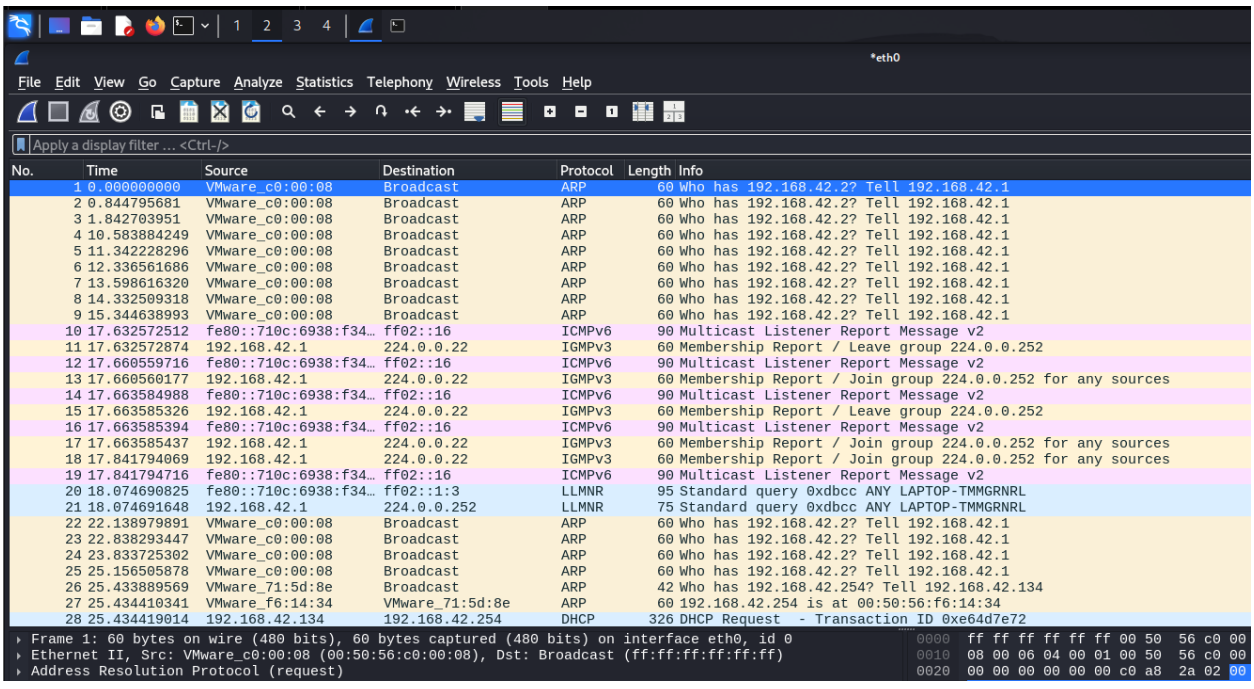
Host list



Sniff Traffic

Ettercap captures the victim's traffic.





Results :-

- Captured login credentials sent via HTTP (unencrypted websites)
- Session cookies that can be used for session hijacking
- Victim traffic redirected to a malicious site (phishing attack)

Conclusion:-

MITM attacks highlight the risks of using insecure communication protocols.
To defend against MITM attacks, organizations and users should:

- Use encrypted connections (HTTPS, TLS, SSH, VPN)
- Enable ARP spoofing protection
- Apply intrusion detection systems
- Educate users about fake certificates and phishing sites