DHCP Attack Using Hyenae

BY MEENU HANDA

WARNING

- This project is conducted strictly for educational and ethical research purposes.
- All testing, scanning, and analysis should be performed only on systems and networks you own or have explicit permission to test.
- Unauthorized activities may violate legal regulations and ethical guidelines.
- Always follow responsible disclosure practices, respect privacy laws, and ensure compliance with relevant cybersecurity policies.

AGENDA

- Objective
- Requirements and Configuration of tools.
- Introduction of Hyenae and Installation steps in window or Linux .
- DHCP attack using Hyenae
- Conclusion
- References
- Thank you

OBJECTIVE

The objective of this project is to understand and demonstrate a DHCP starvation attack using Hyenae. The attack aims to exhaust available IP addresses in the DHCP pool by flooding DHCP requests, thereby preventing legitimate devices from obtaining IP addresses.

Requirements & Configuration

Tools Required:

- **Hyenae** (Hybrid Network Attack Tool)
- **Windows Server** (DHCP Server role configured)
- **Wireshark** (For monitoring network traffic)

Configuration:

- Ensure DHCP Server is running on a Windows Server.
- Install Hyenae.
- The attacker machine should be connected to the same network as the DHCP Server.

What Is DHCP And How Does It Work?

DHCP: Dynamic Host Configuration Protocol is a network protocol used to automatically assign IP addresses and other network configurations (such as subnet mask, default gateway, and DNS servers) to devices on a network. This eliminates the need for manual IP configuration.

How DHCP works?

- DHCP Discovery: When a device (client) connects to a network, it sends a broadcast message (DHCPDISCOVER) to find a DHCP server.

- DHCP Offer: The DHCP server responds with an available IP address and configuration details (DHCPOFFER).

- DHCP Request: The client selects an offer and sends a DHCPREQUEST to confirm its choice.

- DHCP Acknowledgment: The DHCP server acknowledges (DHCPACK) and finalizes the lease of the IP address to the client.

Hyenae and Installation Steps

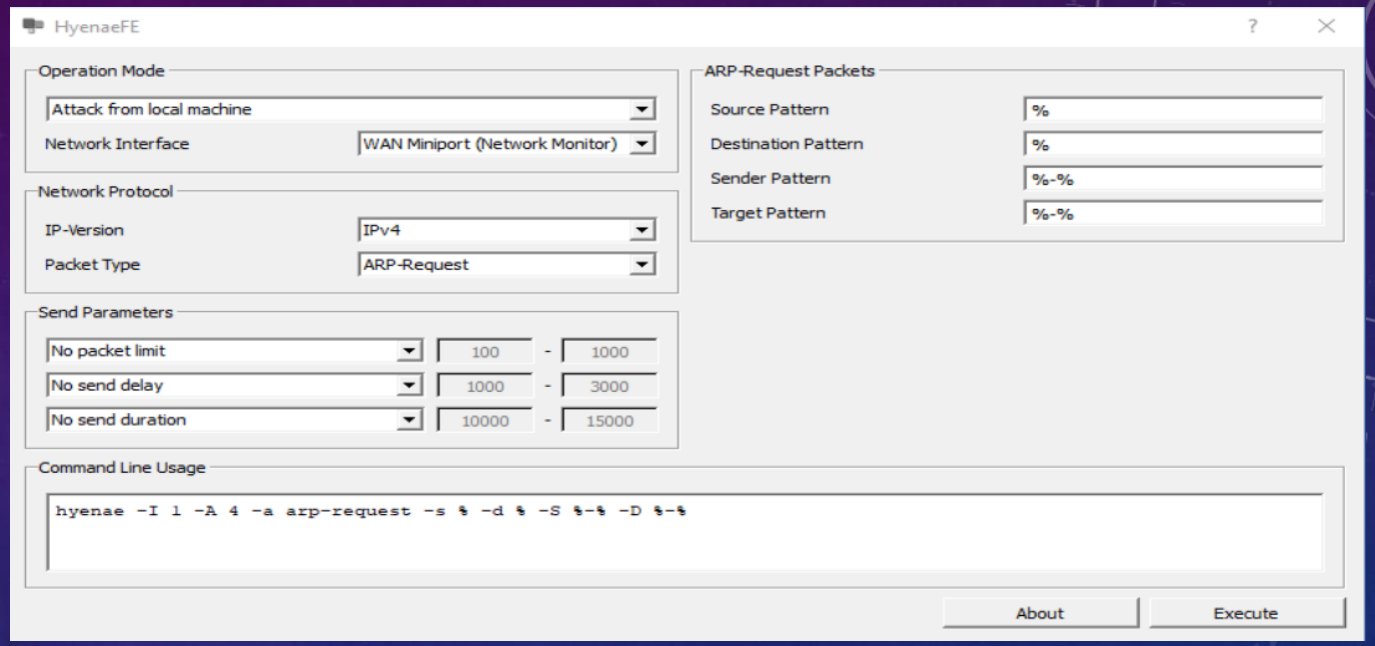
Hyenae is an advanced packet generator that allows for different network attack simulations, including DHCP starvation. It enables attackers to flood the DHCP server with numerous DHCP requests, leading to exhaustion of available IP addresses.

On Windows:

1. Download Hyenae from https://sourceforge.net/projects/hyenae/
2. Check in the destination download folder and double-click on hyenae file to install it.
3. Run Hyenae.

Launch DHCP attack using Hyenae

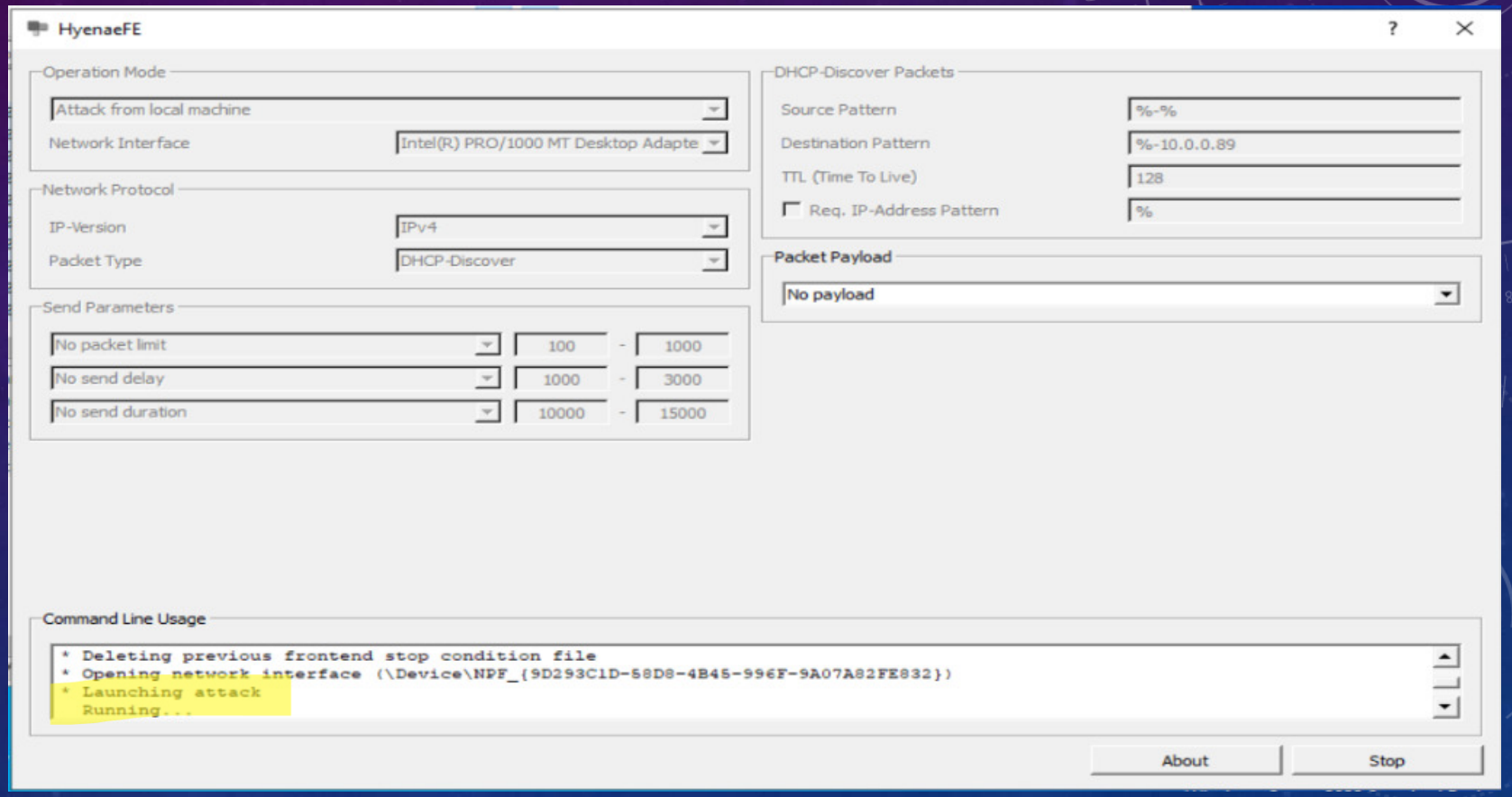
Run Hyenae and configure it for DHCP Attack by selecting following options:



1. Operation mode > Attack from Local Machine.
2. IP-version > IPv4
3. Packet Type > DHCP – Discover
4. Source & Destination Pattern > %-% > 1st % represents MAC Address and 2nd % represents IP Address .
   Since target is windows server (10.0.0.89) where DHCP server is running, replace 2nd % with target IP address.
5. Command Line Usage > represents command.
6. Hit Execute at bottom.

Launch DHCP attack using Hyenae

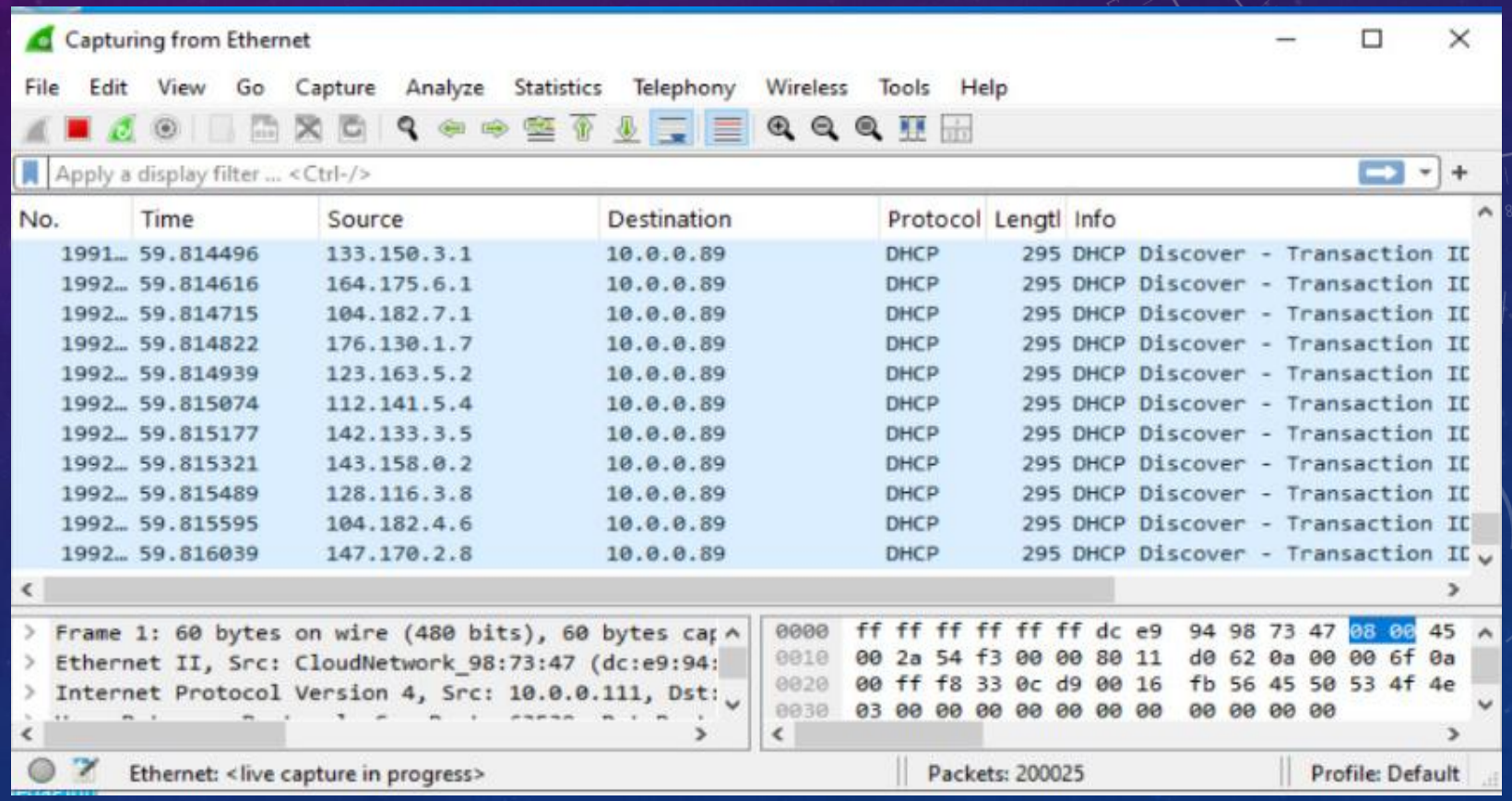
Attack will be launched and simultaneously wireshark will capture packets.



DHCP attack using Hyenae: Capturing traffic using Wireshark

After hitting on execute from hynae tool, traffic captured by wireshark:

DHCP server is hit by DHCP discover packets from random IP addresses.



Conclusion

This project successfully demonstrated how a DHCP starvation attack using Hyenae can exhaust available IP addresses in a network. This highlights the importance of DHCP security measures such as DHCP snooping, rate limiting, and MAC filtering to mitigate such attacks.

References

- https://sourceforge.net/projects/hyenae/
- Youtube: https://youtu.be/FPagUMOzZEE?si=039EUBffdxXfGD2O

Thank you