**Denial of Service and Man-in-the-Middle Attacks**

**Table of contents**

[1. Introduction 1](#_Toc198003423)

[2. Materials 1](#_Toc198003424)

[3. Methodology 1](#_Toc198003425)

[3.1 DoS Attack (hping3) 1](#_Toc198003426)

[3.2 MiTM Attack (Ettercap) 7](#_Toc198003427)

[4. Results 9](#_Toc198003428)

[5. Discussion 9](#_Toc198003429)

[6. Conclusion 9](#_Toc198003430)

[7. References 9](#_Toc198003431)

# 1. Introduction

This report describes my procedures for Attack and How It Works (Denial of Service DoS, Man-in-the-Middle MiTM attack with Kali Linux virtual machine and Windows 10 virtual machine) using hping3 for DoS to flood the target host when I was taking Ettercap (MiTM) as well to sniff network traffic. It was an attempt to learn more about these kinds of attacks and their actual implications while practicing ethical hacking.

# 2. Materials

* Kali Linux VM (Attacker, IP: 192.168.24.128)
* Windows 10 VM (Victim, IP: 192.168.24.139)
* Second Kali Linux VM (MiTM, IP: 192.168.24.157)
* Tools: hping3, Ettercap, Wireshark
* Virtual network environment

# 3. Methodology

## 3.1 DoS Attack (hping3)

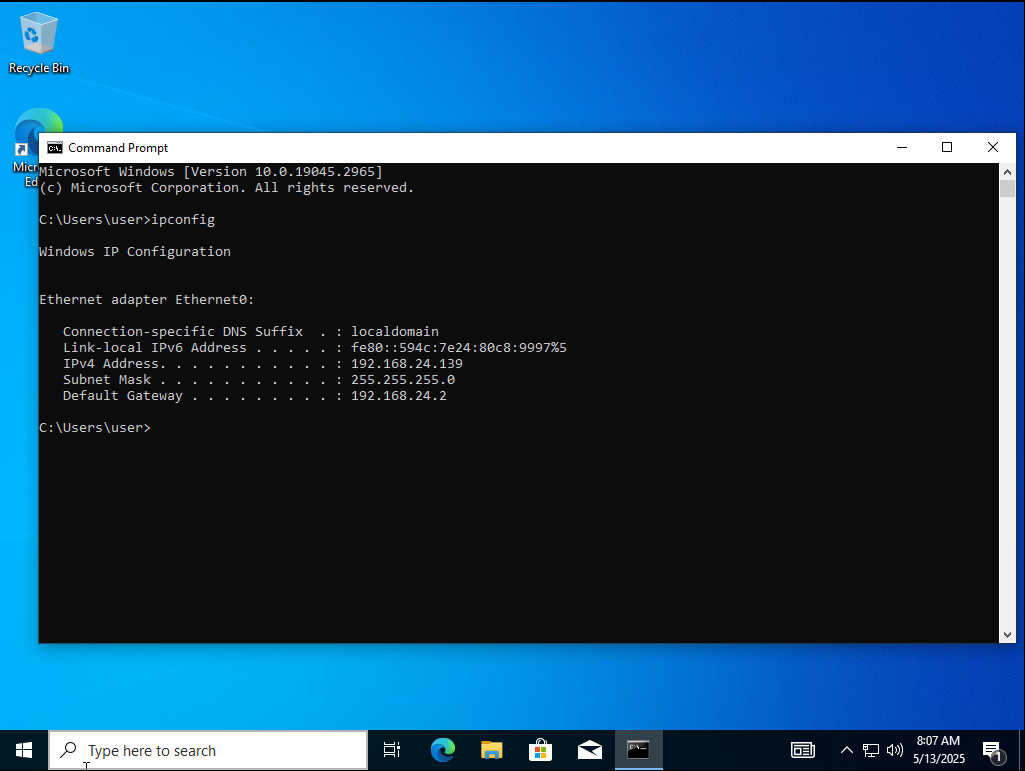
The DoS attack is set to SSH hping3 TCPing3 packets into exhausting resources of the Windows 10 VM.

1. **Setup**:
   * Launched Kali Linux VMs (IPs: 192.168.24.128 – kali, 192.168.24.139 – Win 10 IP).
   * Verified IP addresses using (ip address) on Kali and ipconfig on Windows.

Screenshot 1:

A screenshot of a computer

AI-generated content may be incorrect.



* + Disabled the Windows firewall to ensure connectivity and tested with a ping command.

Screenshot 2:

A screenshot of a computer

AI-generated content may be incorrect.

A computer screen shot of a black screen

AI-generated content may be incorrect.

1. **Port Scanning**:
   * Executed sudo hping3 --scan 1-65535 192.168.24.139 -S as root to identify open ports on the victim machine.

Screenshot 3:

A screenshot of a computer

AI-generated content may be incorrect.

1. **Baseline Observation**:
   * Monitored the Windows 10 VM’s resource usage (CPU, memory, network) in Task Manager prior to the attack.

Screenshot 4:

A screenshot of a computer

AI-generated content may be incorrect.

1. **Initial DoS Attack**:
   * Ran hping3 -S 192.168.24.139 -p 3389 --flood to flood port 3389 (RDP) with SYN packets.

Screenshot 5:

A screenshot of a computer

AI-generated content may be incorrect.

* + Observed the impact on the victim’s resource consumption.

Screenshot 6:

A screenshot of a computer

AI-generated content may be incorrect.

* + Terminated the attack using Ctrl+C.

1. **Enhanced DoS Attack**:
   * Executed hping3 -c 200000 -d 140000 -S -p 3389 --flood --rand-source 192.168.24.139 to amplify the attack with larger packets and spoofed source IPs.

Screenshot 7:

A screenshot of a computer

AI-generated content may be incorrect.

* + Recorded the resulting resource spikes.

Screenshot 8:

A screenshot of a computer

AI-generated content may be incorrect.

## 3.2 MiTM Attack (Ettercap)

The MiTM attack used ARP poisoning to intercept traffic between Windows 10 VM and the second Kali VM.

1. **Setup**:
   * Launched two Kali VMs (192.168.24.128 and 192.168.24.157) and the Windows 10 VM (192.168.24.139).
   * Opened Ettercap’s graphical interface on the attacker Kali (192.168.24.128) and selected the appropriate network interface.

Screenshot 9:

A screenshot of a computer

AI-generated content may be incorrect.

1. **Host Discovery**:
   * Host scan in Ettercap to scan the devices on network and assigning IPs like executed by the Ettercap o 192.168.24.139,192.168.24.157
2. **Target Selection**:
   * Set Windows 10 VM (192.168.24.139) as TARGET 1 and next Kali VM (192.168.24.157) in Ettercap as TARGET 2.

Screenshot 10:

A screenshot of a computer

AI-generated content may be incorrect.

1. **ARP Poisoning**:
   * Enabled ARP poisoning in Ettercap, selecting “Sniff remote connections” to capture traffic.
   * Ran Wireshark concurrently to monitor and analyze the intercepted packets.

Screenshot 11:

A screenshot of a computer

AI-generated content may be incorrect.

# 4. Results

* **DoS Attack**: The hping3 scan identified open ports, including port 3389, on Windows 10 VM. The initial attack caused a moderate increase in CPU and network usage. The enhanced attack, with larger packets and randomized source IPs, significantly intensified resource consumption, demonstrating the impact of aggressive flooding. Disabling the firewall ensured packet delivery.
* **MiTM Attack**: Ettercap successfully enumerated network devices. ARP poisoning enabled the interception of traffic between the Windows 10 VM and the second Kali VM, with Wireshark confirming the capture of packets. Proper interface selection was crucial for effective execution.

# 5. Discussion

In this case the DoS demonstrated how systems can be vulnerable to resource exhaustion; thus, intrusion prevention systems were needed. The MiTM attack illustrated the dangers of unsecured traffic and the issue of the necessity of secure communication to be on the safe side. In both experiments, they were performed in a lab to be ethical and not cause real-world harm.

# 6. Conclusion

Successfully demonstrated the execution of DoS and MiTM attacks using hping3 and Ettercap. The activities provided a deeper understanding of attack methodologies and the critical role of cybersecurity measures. All steps were thoroughly documented to reflect my engagement with the lab objectives.

# 7. References

* Guide Video: <https://www.youtube.com/watch?v=S9FdzDXgniA>