A Project Abstract on

Gaining Access And performing Attacks Using Kali-Linux

### Network Protocols and Security(23EC2210A)

Submitted by

Karthik B -2320040057

Venkata Ram charan -2320040017

#### of Section 7

Under the guidance of

**Shaik Asif**



**Abstract:**

This research paper aims to explore the feasibility and potential impact of two distinct cyber threats targeting Windows 10 systems:

crashing the operating system and executing a man-in-the-middle (MITM) attack. Both techniques utilize Kali Linux, a popular penetration testing platform, to exploit vulnerabilities and compromise system integrity.

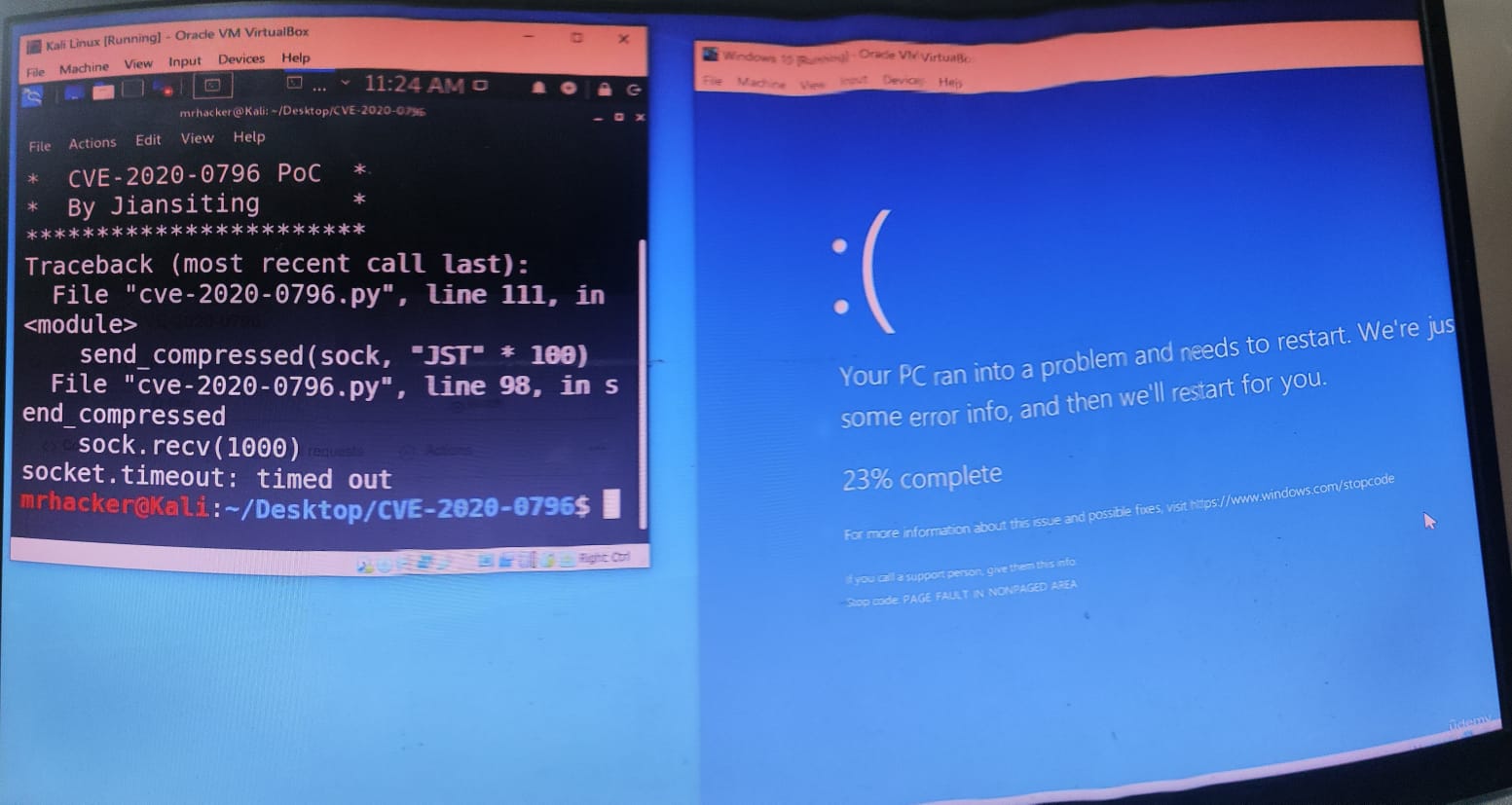
Windows 10 Crashing: The first part of this study investigates methods to induce system crashes on Windows 10. This can be achieved through various techniques, such as:

Memory exhaustion: Overloading the system's memory with excessive processes or data.

Blue Screen of Death (BSOD) triggers: Exploiting known vulnerabilities or programming errors to force a system crash.

Kernel-level attacks: Targeting the core components of the operating system to destabilize its operation.

Man-in-the-Middle Attacks: The second part of this research focuses on MITM attacks, where an attacker intercepts and manipulates communication between two parties. This can be accomplished using:

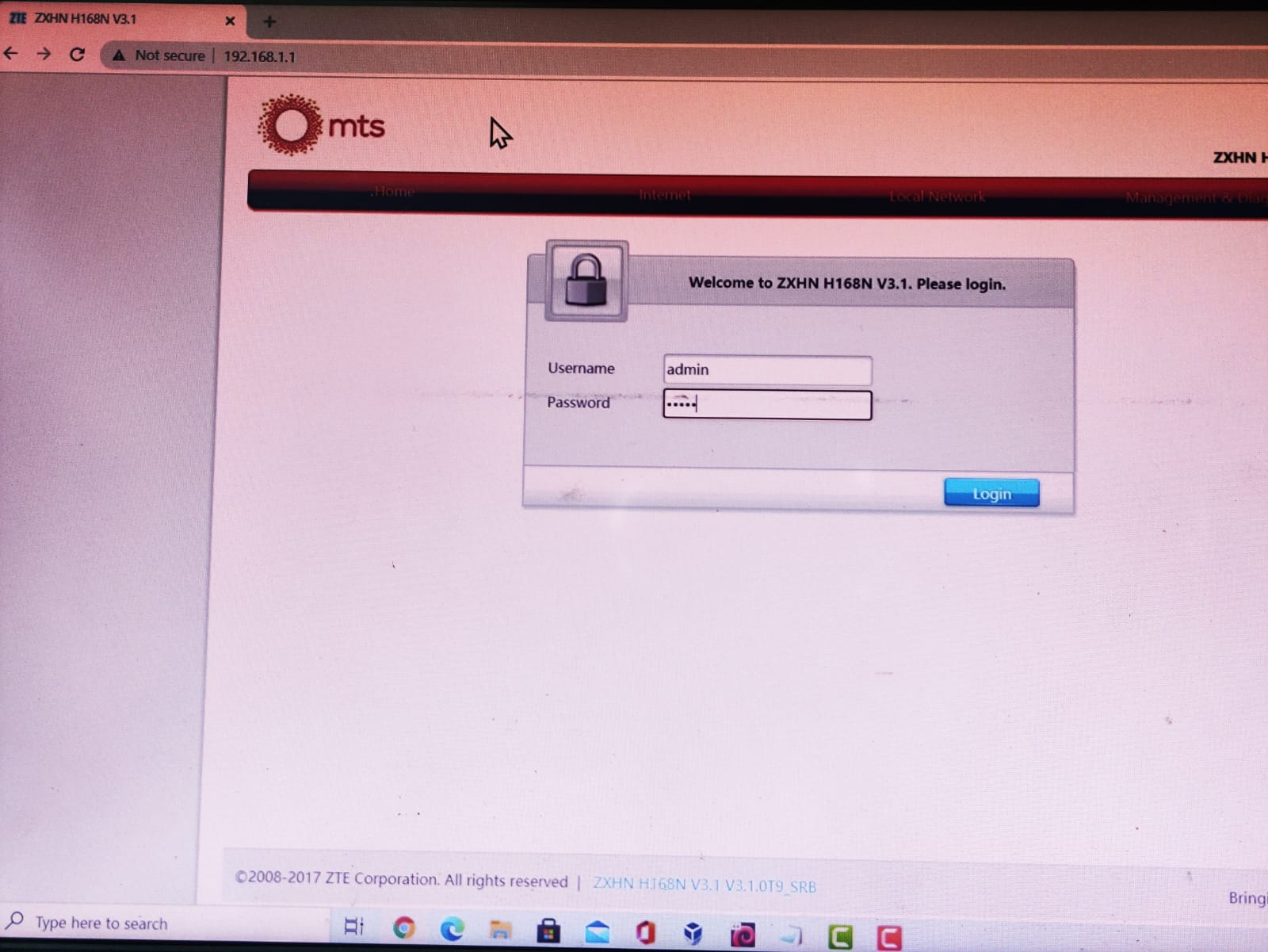


ARP poisoning: Manipulating the Address Resolution Protocol (ARP) cache to redirect network traffic through the attacker's system.

DNS spoofing: Intercepting and modifying DNS requests to redirect users to malicious websites.

SSL/TLS interception: Intercepting and decrypting encrypted traffic, compromising the security of online communications.

Comparison and Analysis: The paper will compare and analyze the effectiveness, potential impact, and detection methods for both types of attacks. Key factors to be considered include:



Technical complexity: The level of expertise required to execute the attacks.

Impact on system availability: The potential consequences of system crashes and compromised data.

Detection and mitigation strategies: Techniques to identify and prevent these attacks.

**Conclusion:**

This research aims to provide a comprehensive understanding of the vulnerabilities and potential risks associated with Windows 10 systems. By exploring techniques for crashing Windows 10 and conducting MITM attacks using Kali Linux, this study seeks to contribute to security awareness and help organizations implement effective countermeasures to protect their systems and data.