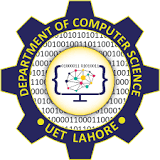
**LAB REPORTS**



**Session 2023-2027**

**Submitted by:**

Sumaira Hafeez 2023-CS-1

**Supervised by:**

Dr. Faiza

**Course:**

Information Security

**Department of Computer Science**

**University of Engineering and Technology,**

**Lahore Pakistan**

Contents

[**TASK 4 CASE STUDY WANNACRY RANSOMEWARE ATTACK** 3](#_Toc188788009)

[**1.** **Introduction:** 3](#_Toc188788010)

[**2.** **Assets Targeted:** 3](#_Toc188788011)

[ **Corporate data and files:** 3](#_Toc188788012)

[ **Systems and networks:** 3](#_Toc188788013)

[**3.** **Vulnerabilities Exploited:** 3](#_Toc188788014)

[**4.** **Threat Agents Involved:** 3](#_Toc188788015)

[**5.** **Impact on the Organization:** 3](#_Toc188788016)

[**6.** **CONCLUSION:** 4](#_Toc188788017)

# **TASK 4 CASE STUDY WANNACRY RANSOMEWARE ATTACK**

## **Introduction:**

The WannaCry ransomware attack, which occurred in May 2017, is one of the most infamous cyberattacks in recent history. The ransomware spread across the globe, affecting hundreds of thousands of computers in over 150 countries. It encrypted files on infected systems and demanded ransom payments in Bitcoin, severely disrupting operations for organizations worldwide.

## **Assets Targeted:**

The primary assets targeted by the ransomeware was:

### **Corporate data and files:**

WannaCry encrypted files on infected systems, preventing access to critical business data.

### **Systems and networks:**

Computers running Microsoft Windows, especially those that were not updated with the latest security patches.

* **Health care organizations:**

Specifically, the UK's National Health Service (NHS), where operations were disrupted, including surgeries and patient care.

## **Vulnerabilities Exploited:**

The attack took advantage of a critical vulnerability in Windows systems known as **EternalBlue**. This vulnerability allowed attackers to remotely execute code on unpatched machines. The vulnerability had been disclosed by the NSA (National Security Agency) and was later leaked by the hacking group **Shadow Brokers**. WannaCry spread quickly because many organizations had not applied the security patch (MS17-010) released by Microsoft in March 2017.

## **Threat Agents Involved:**

The threat agents responsible for the WannaCry attack were linked to the **Lazarus Group**, a cybercrime group believed to be associated with North Korea. This group has been known for carrying out a variety of cyberattacks, including financial theft, espionage, and ransomware attacks. The use of the EternalBlue exploit made it easier for the attackers to spread the ransomware quickly and widely.

## **Impact on the Organization:**

The impact of the WannaCry attack on organizations was significant:

* **Disruption of services:** Critical services, especially in healthcare, were interrupted. For example, the NHS in the UK faced severe disruptions, with some hospitals unable to access patient records or perform surgeries.
* **Financial losses:** The attack led to financial losses due to system downtime, ransom payments, and recovery costs. It is estimated that WannaCry caused damages amounting to billions of dollars globally.
* **Reputation damage:** Organizations that were affected by the attack suffered reputational damage. The inability to protect systems from such a widespread attack led to a loss of trust from customers and partners.
* **Data loss:** Some organizations suffered data loss because the encrypted files could not be restored without paying the ransom or recovering from backups, which were often not up-to-date.

# **CONCLUSION:**

The WannaCry attack highlights the critical importance of patching and updating systems regularly to protect against known vulnerabilities. It also serves as a reminder of the potential devastating effects of ransomware and other cyberattacks on businesses and essential services. The incident prompted governments and organizations worldwide to improve cybersecurity protocols and take proactive steps to prevent similar attacks in the future.