**Name:** Hemant Jain

**Lab Progress Report Due Date:** 2/01/2021

**Current Week Since Start Date:** Week 3 (2/01/2021– 2/08/2021)

**Reporting Week:** From Jan 26, 2021 to Feb 01, 2021

**Summary about the TestOut Module-1 Learning:**

From the TestOut LabSim Security Threats, Attacks and Vulnerabilities Section, I got to learn about Internal threat agents are authorized individuals that carry out an attack by exploiting their inherent privileges. This category includes employees (both current and former), janitors, security guards, and even customers. External threat agents are individuals or groups that attack a network from the outside and seek to gain unauthorized access to data.

The goal of persistent threat was to gain access to a network and retain access undetected. With this type of threat, attackers go to great lengths to hide their tracks and presence in the network. Before carrying out an attack, a threat actor typically gathers open-source intelligence (OSINT) about the target. I learnt about the different types of Threat Actors namely Insider, White Hat, Black Hat, Gray Hat, Script kiddie, Hacktivist, Organized Crime, Nation state, Competitor. I learnt how the hacker term is defined and who is called hacker.

Learnt about the various general attack strategies incorporated namely like Reconnaissance which is the process of gathering information about an organization, including the system hardware, network configuration. Learnt how the social engineering tactically manipulates the others into providing the sensitive information. Gained insights about the technical approaches, breaching the system and knowing what the penetration of system defenses offers and what are the various possible breaching preventive measures. How the escalation of the privileges is the primary objective of the attacker. Learnt about the backdoor and how it stands as an alternative method in accessing an application or OS for troubleshooting. Read about the methodologies ranging from Layering, Principle of least privileges, Variety, randomness, simplicity.

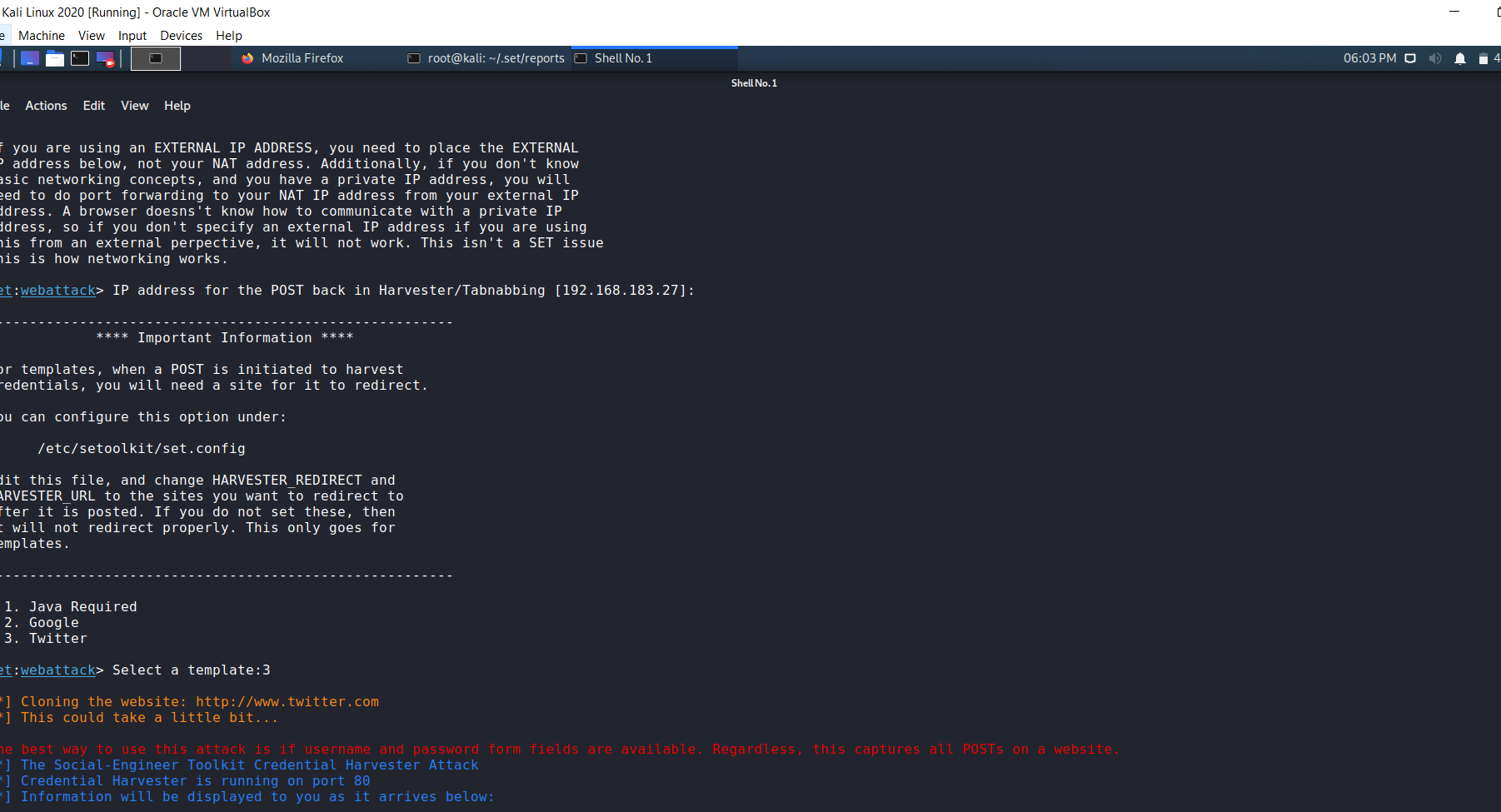
I read about the fileless virus which uses legitimate programs to infect a computer. A worm which is a self-replicating program and does not require a host file to propagate. A trojan horse which is a malicious program this is disguised as legitimate or desirable software and cannot replicate itself. A malware infected computer that allows remote software updates and control by a command-and-control center is a zombie and has a zombie master. Malware is software designed to infiltrate or damage a computer system without the owner’s consent or knowledge. Some malware even takes control of the computer system. How Malware can attempt to hide itself. Social engineering which refers to an attacker enticing or manipulating people to perform tasks or relay information. In social engineering, hacker tries to get a person to do something the person would not do under normal circumstances. Social engineering process phases like research, development, exploitation. Conceptualized about the manipulation types like moral obligation, innate human trust, threatening, offering something for very little to nothing and ignorance.

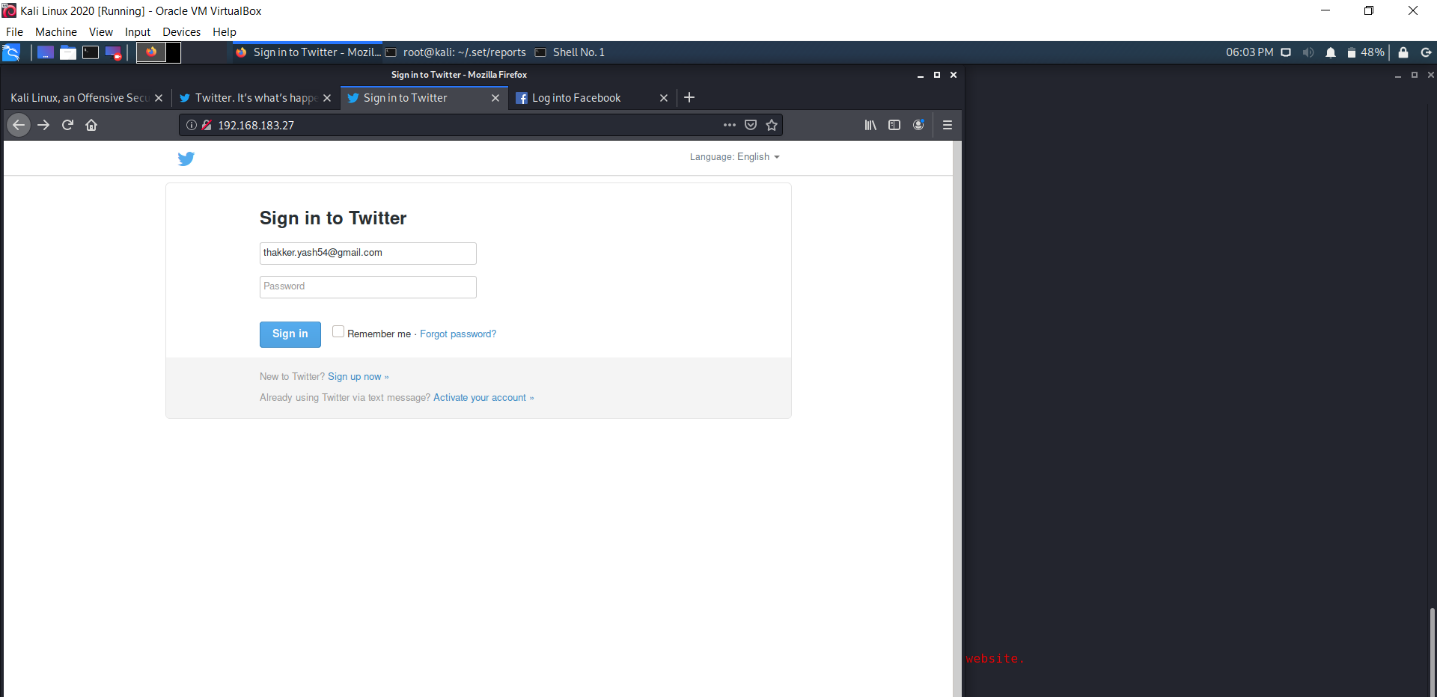
Read about the two types of the attacks: Opportunistic and Targeted, what are the various tactics for the elicitation which is a technique used to extract information from a target with arousing suspicion. How social engineering involves pretexting, preloading and impersonation. Users interfacing with the internet either through email or browsing websites can pose substantial security threats to an organization.

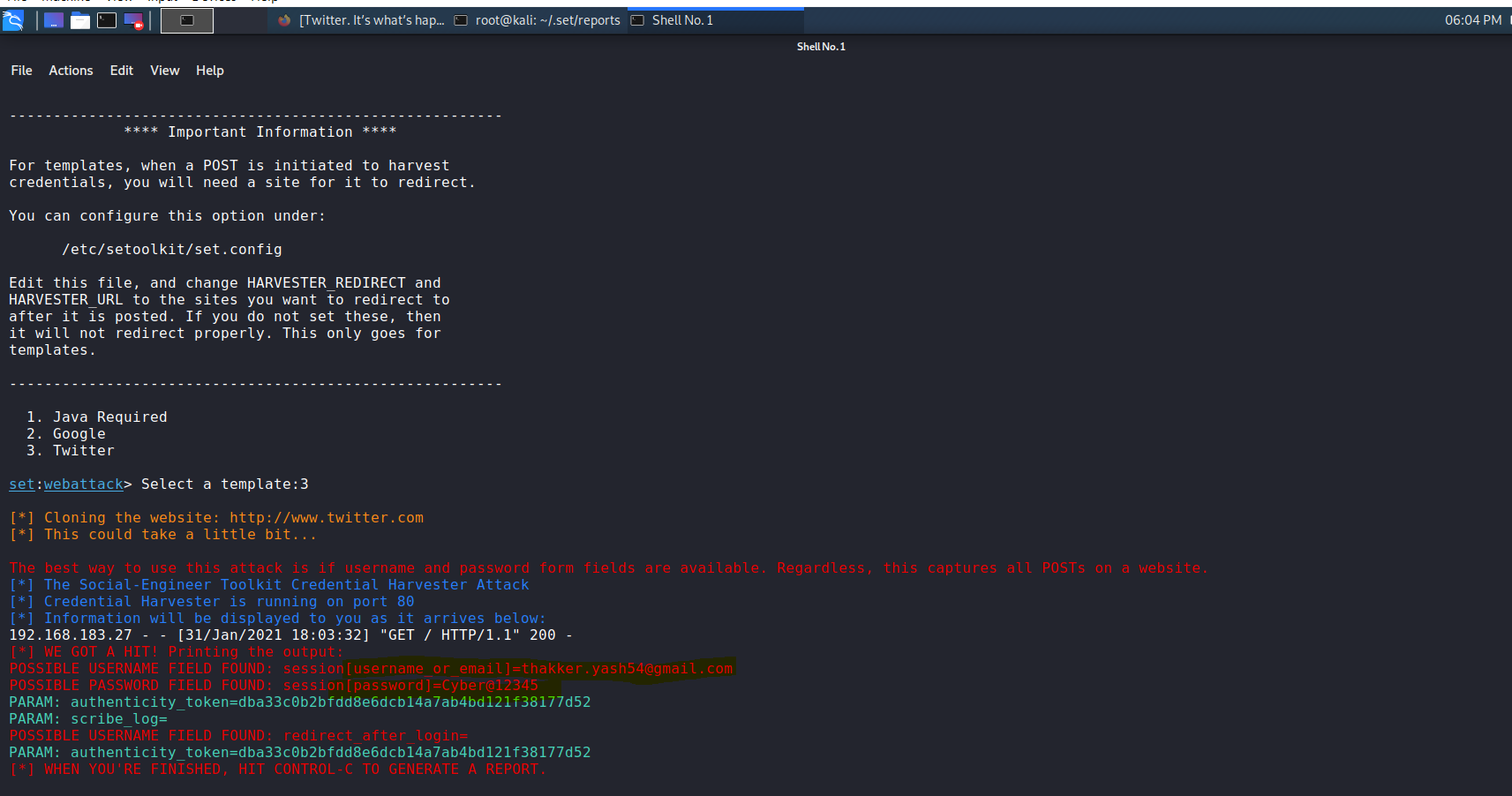
Attacks that entice users to provide sensitive information or to click a link that installs malware are called social engineering attacks. For the organization’s overall security, we need to increase user awareness of the types of threats and how to avoid them is critical. Different vulnerabilities in Network like Default accounts and passwords, Weak Passwords, Privilege escalation, backdoor, cloud-based, and third-party systems, inherent vulnerabilities, application flaws, misconfigurations, root account. To avoid unnecessary risk, use the root account only when necessary. This includes experienced administrators. The primary cause of misconfiguration is human error. Flaws in the validation and authorization of users present the greatest threat to security in transactional applications.

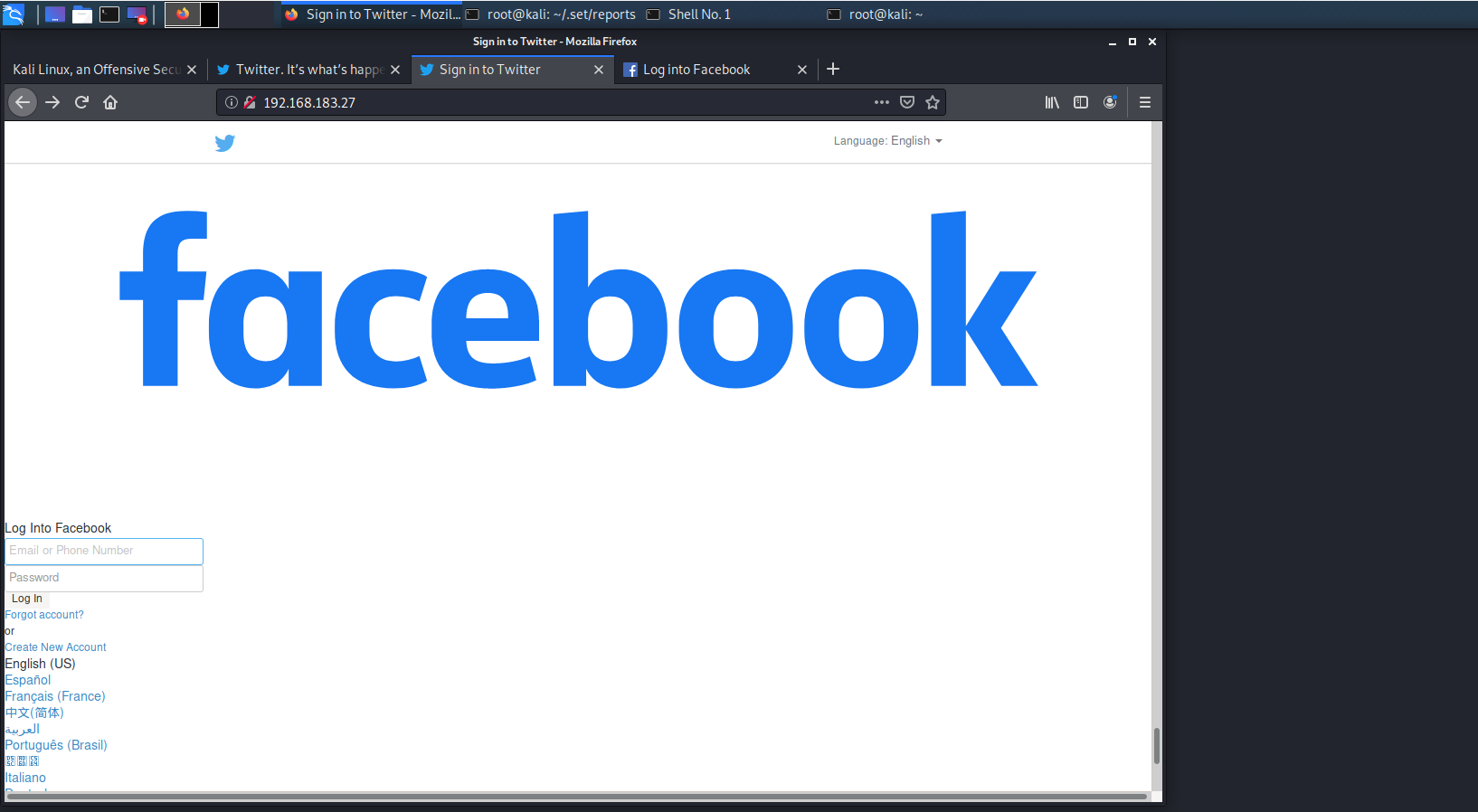
Intrigues by the different types of motivation techniques like Authority and Fear, Social Proof, Scarcity, Likeability, Urgency, Common ground, and shared interest. Learnt about the various types of attackers like Insiders, Hackers and Nation state. Vulnerabilities in networks and systems are often exploited by attackers. Impact analysis of the Data loss, data breach, data exfiltration, identity theft, and availability loss. Various types of the phishing attacks in the social engineering attacks like Spear phishing, whaling, vishing and SMS phishing and others like Pharming and Social Networking.

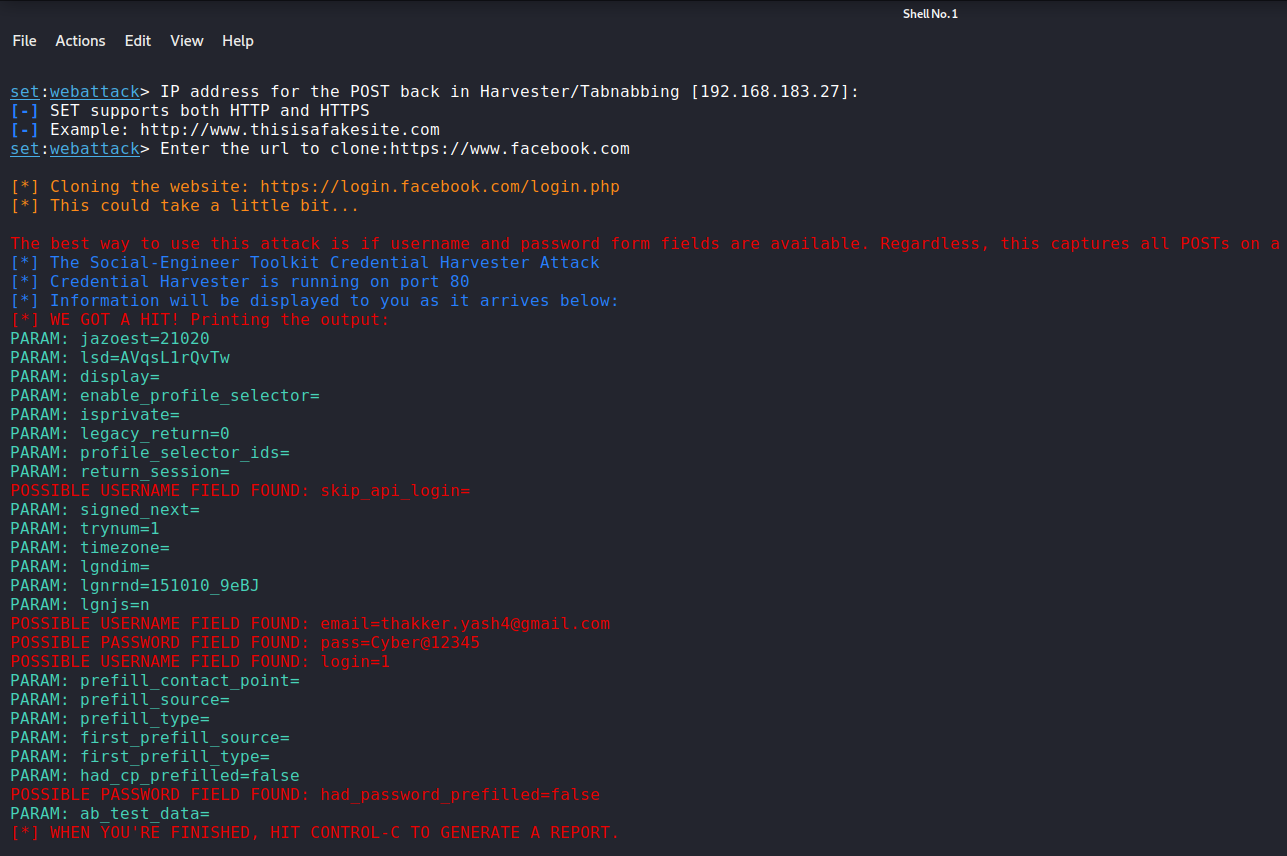
**In-class Lab Homework:**

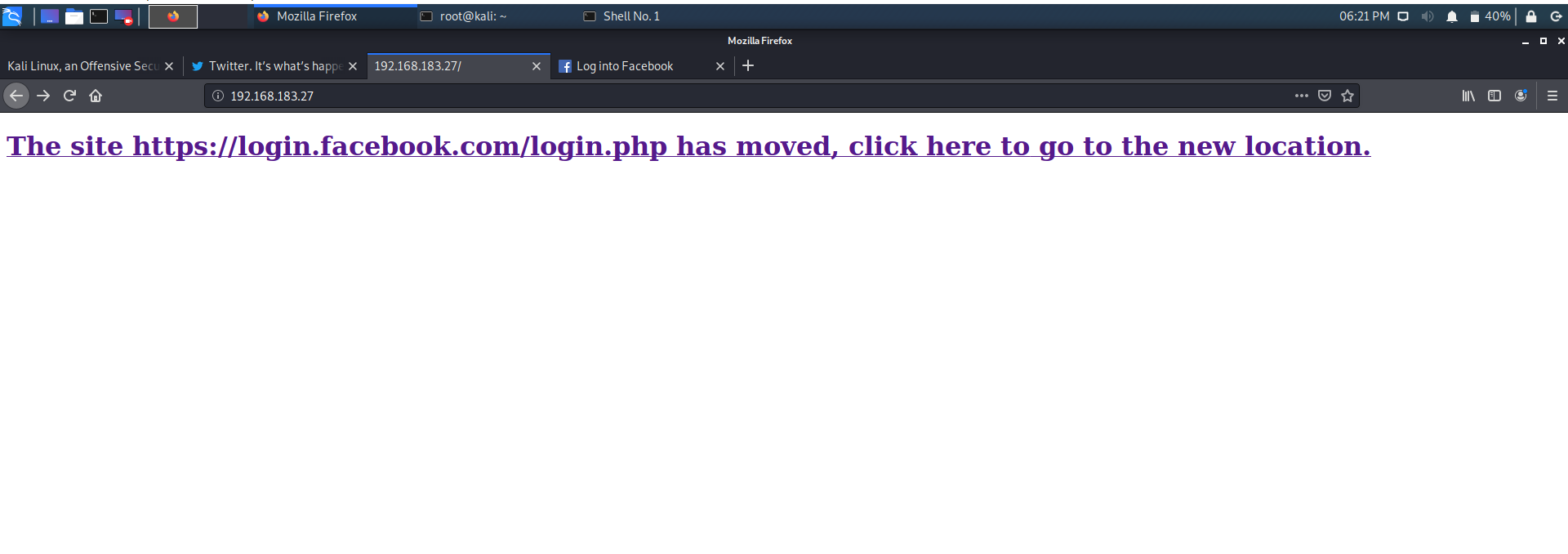
****

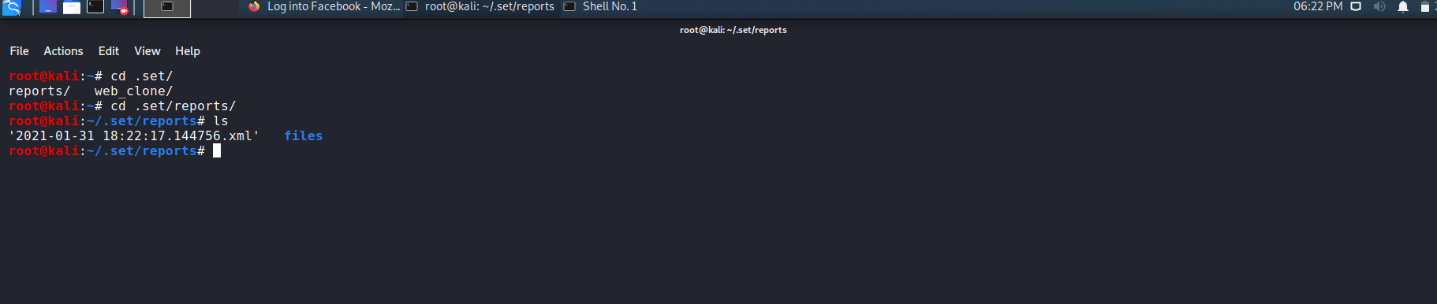
****

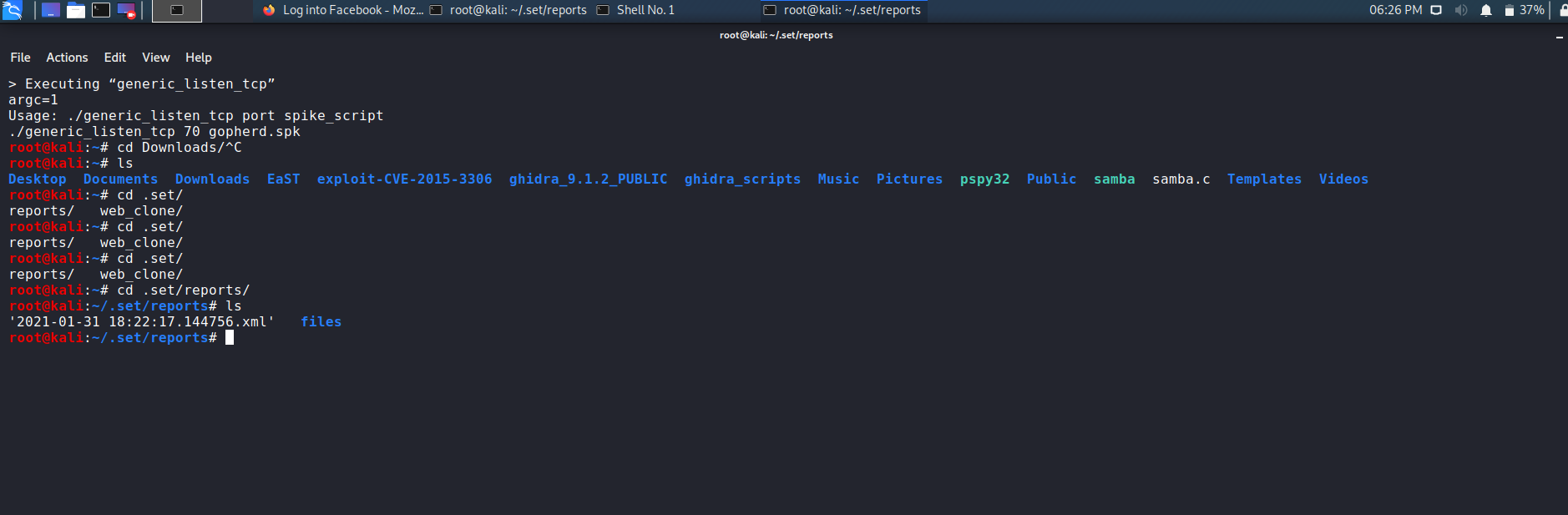
****

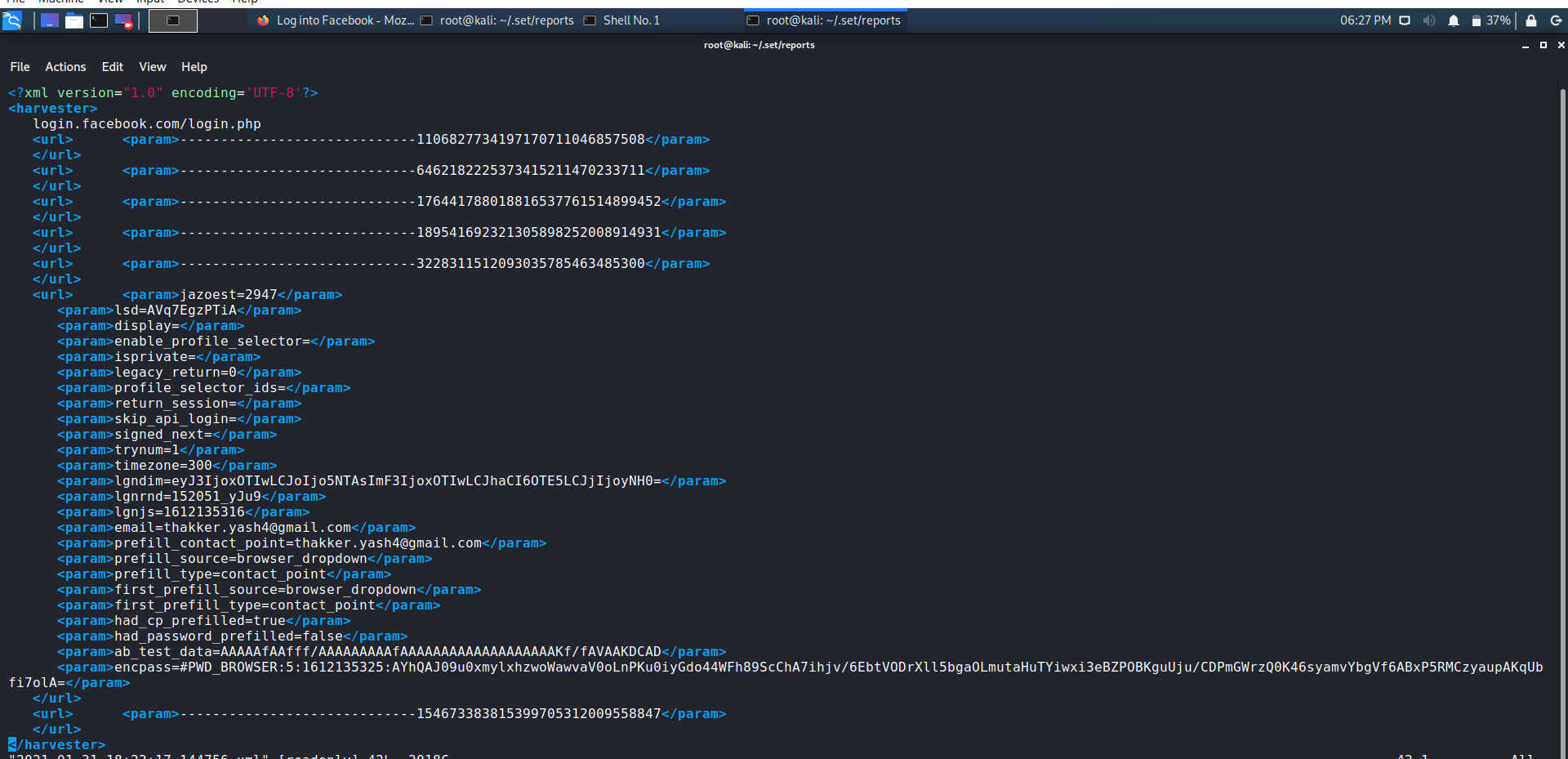
****

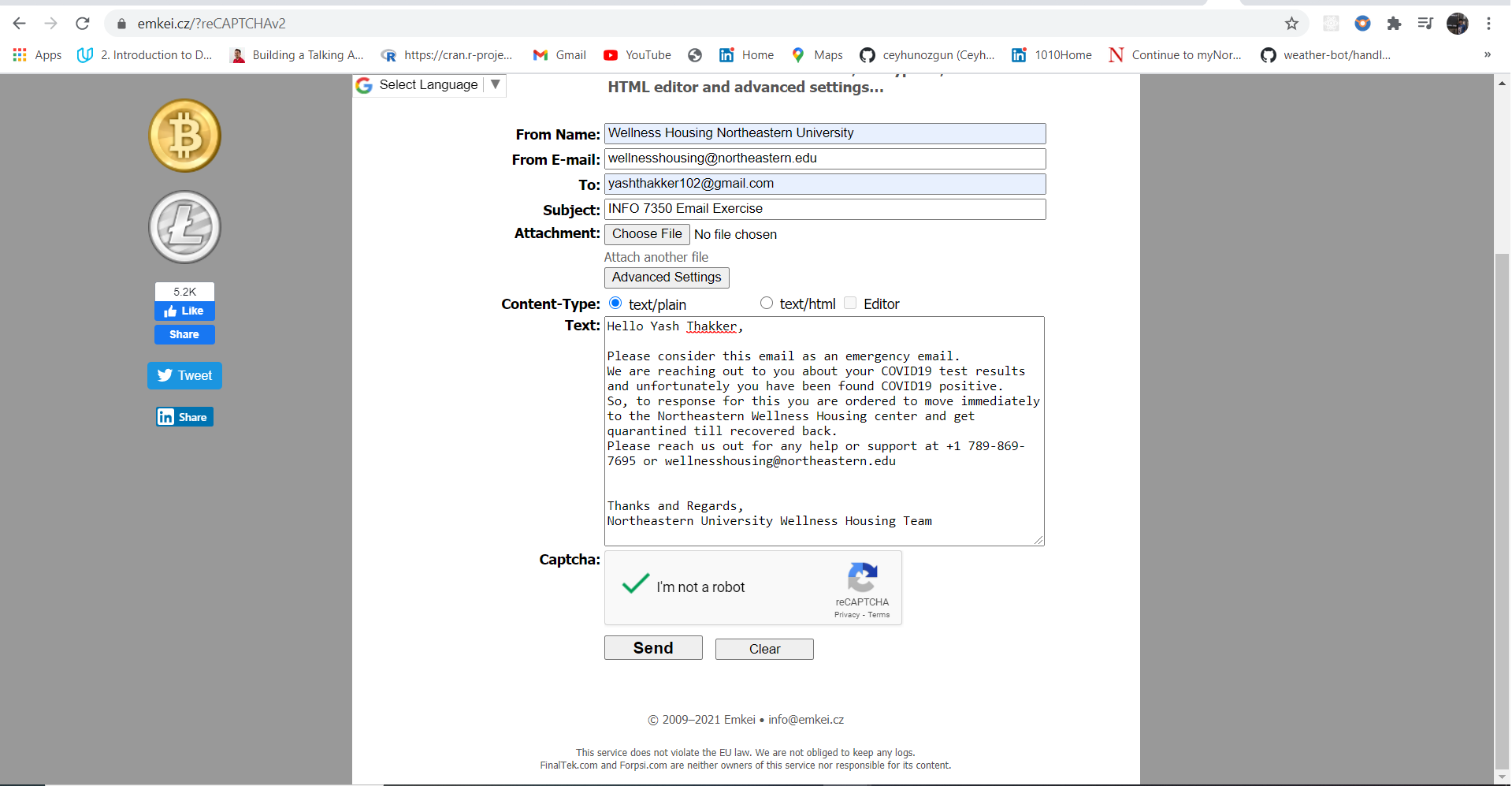
****

****

****

****

****

****

**Progress Embedded Image of Progress Report from LabSim :**

