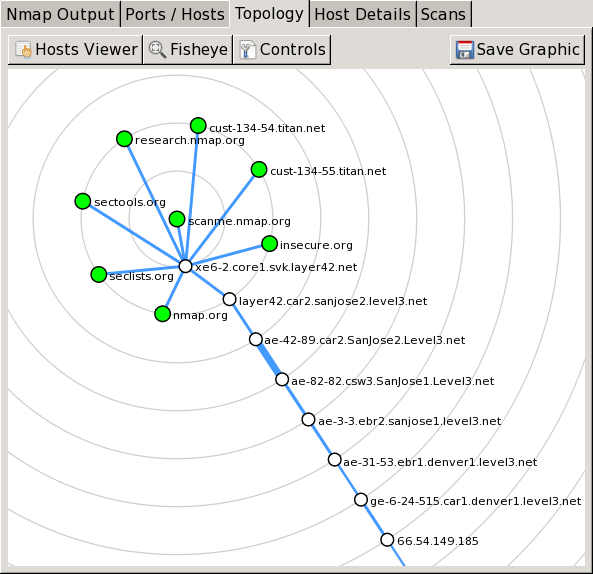
***ASSIGNMENT - 2***

***NAME: SHUBHAM YADAV***

***REG N0 : 21BCE8284***

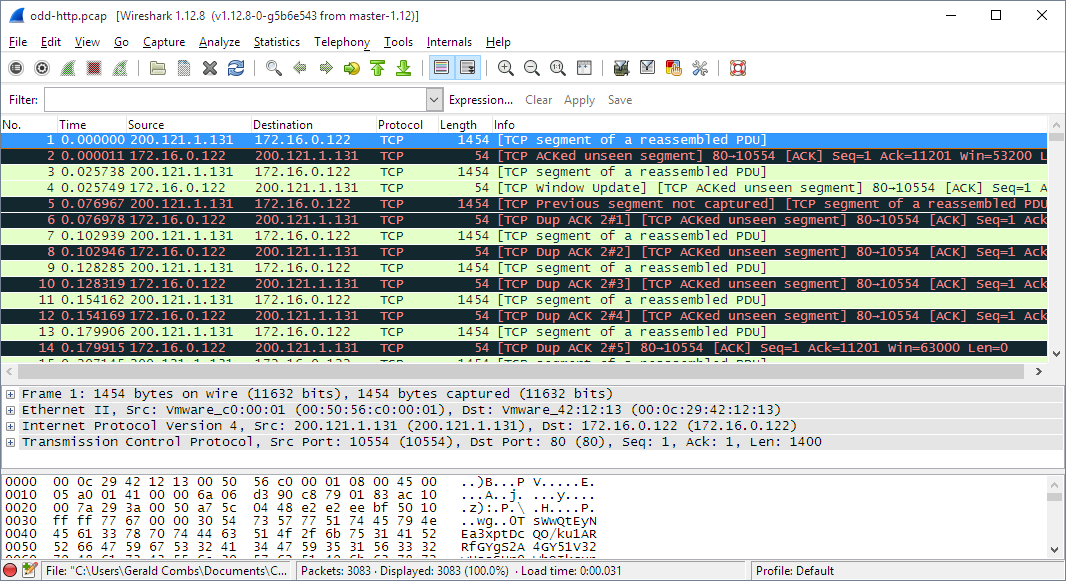
***1. Nmap (Network Mapper):***

*Nmap is a versatile network scanning tool that serves as a Swiss army knife for network reconnaissance. It allows security professionals and ethical hackers to discover hosts, identify open ports, detect services, and even fingerprint operating systems. Nmap's scriptable capabilities make it highly adaptable for various scanning tasks, from basic network discovery to vulnerability assessment.*

**

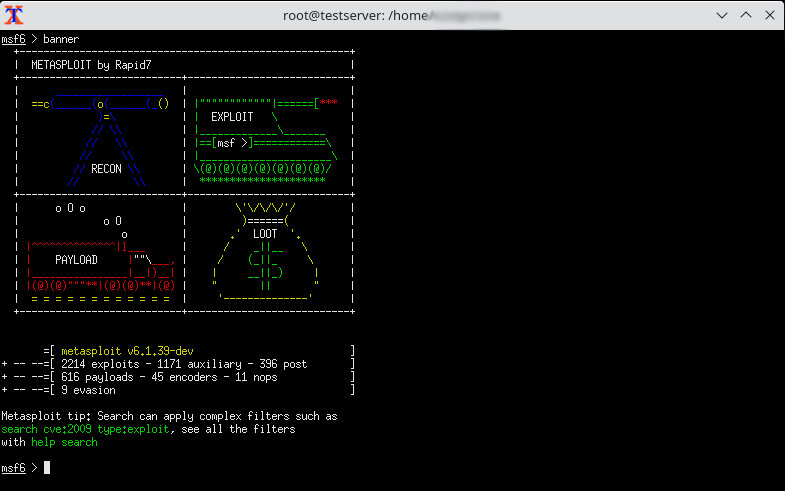
***2. Wireshark:***

*Wireshark is an indispensable tool for deep packet inspection and network traffic analysis. It provides a graphical interface for capturing and dissecting network packets, making it easier to troubleshoot network issues, analyze protocols, and uncover potential security vulnerabilities. Security experts rely on Wireshark to gain insights into network communications and identify anomalies.*

**

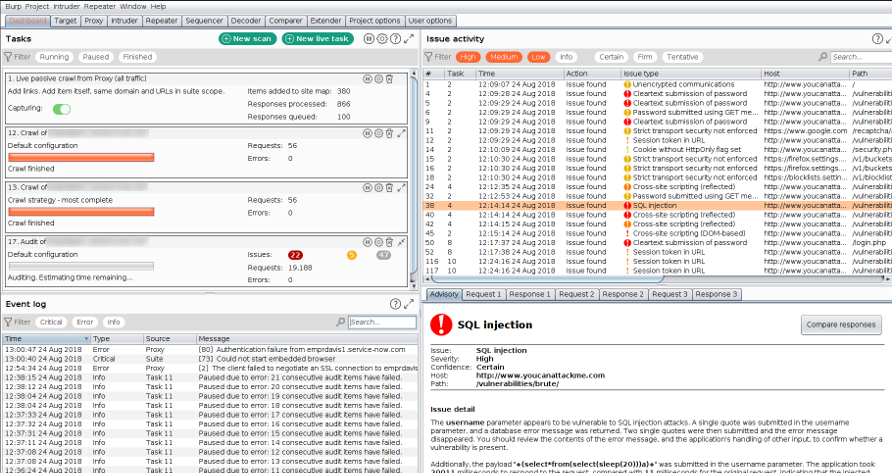
***3. Metasploit Framework:***

*The Metasploit Framework is a comprehensive penetration testing and exploitation tool that empowers security professionals to find, exploit, and validate vulnerabilities in target systems. With its vast collection of exploits, payloads, and post-exploitation modules, Metasploit is a must-have for simulating real-world attacks, assessing system security, and hardening defenses.*

**

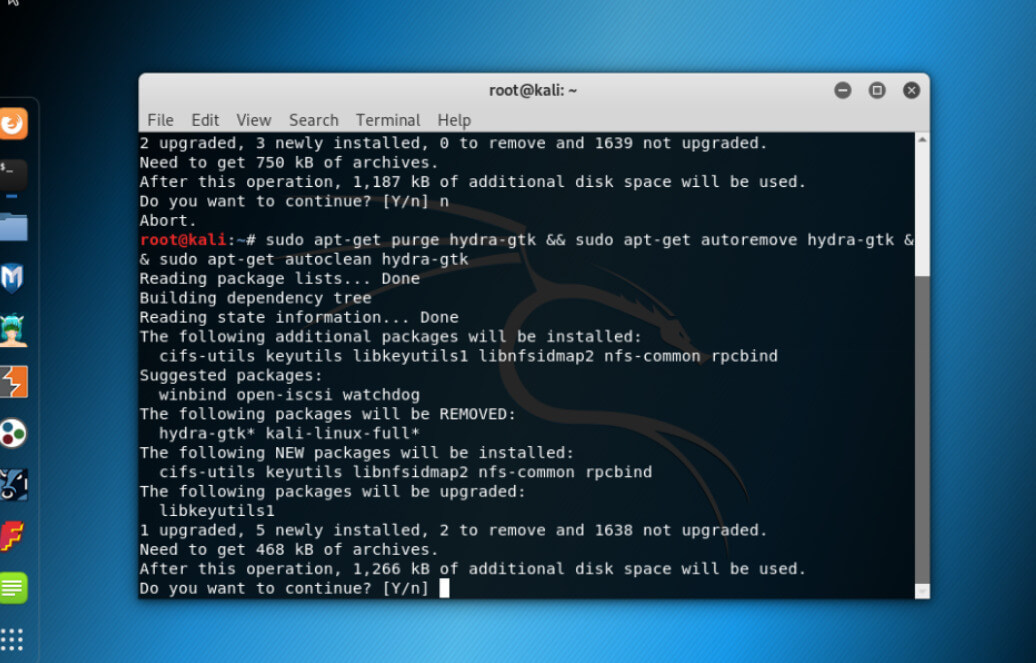
***4. Burp Suite:***

*Burp Suite is a renowned web application security testing tool that combines scanning, crawling, and manual testing capabilities. Security experts use it to identify and validate vulnerabilities in web applications, such as SQL injection, cross-site scripting (XSS), and security misconfigurations. Burp Suite's user-friendly interface simplifies the process of finding and remediating web application security issues.*

**

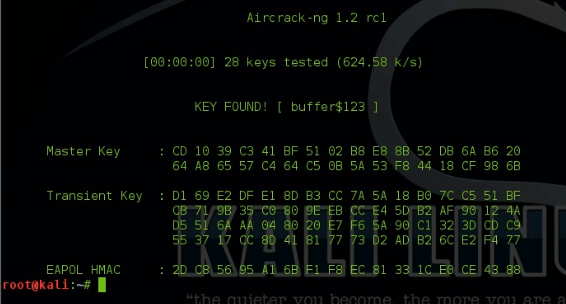
***5. Hydra:***

*Hydra is a potent password-cracking tool known for its versatility and effectiveness. It supports various protocols, enabling security professionals to conduct dictionary and brute-force attacks against services like SSH, FTP, RDP, and more. Hydra is an essential tool for identifying weak or easily guessable passwords and strengthening authentication mechanisms.*

**

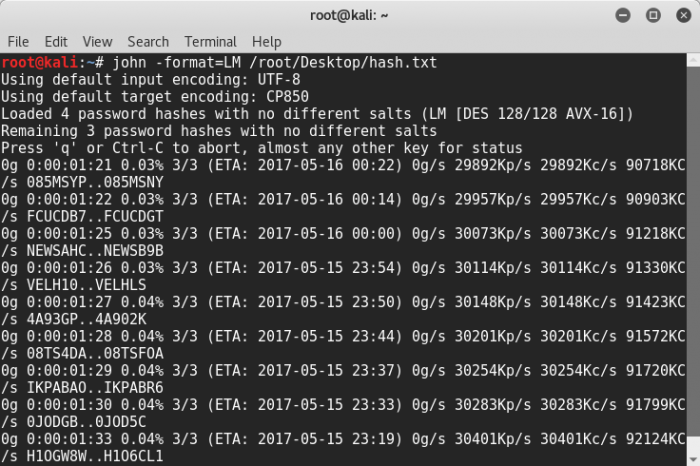
***6. Aircrack-ng:***

*Aircrack-ng is a specialized suite of tools for assessing and securing Wi-Fi networks. It includes utilities for capturing wireless packets, performing WEP and WPA/WPA2 cracking, and conducting dictionary attacks on Wi-Fi passwords. Security testers use Aircrack-ng to evaluate the security of wireless networks and recommend improvements.*

**

***7. John the Ripper:***

*John the Ripper is a renowned password-cracking tool with a focus on Unix-based systems. It supports various password hash algorithms and can perform dictionary attacks and brute-force attacks on password hashes. This tool is indispensable for testing the strength of user passwords and enhancing overall security.*

**

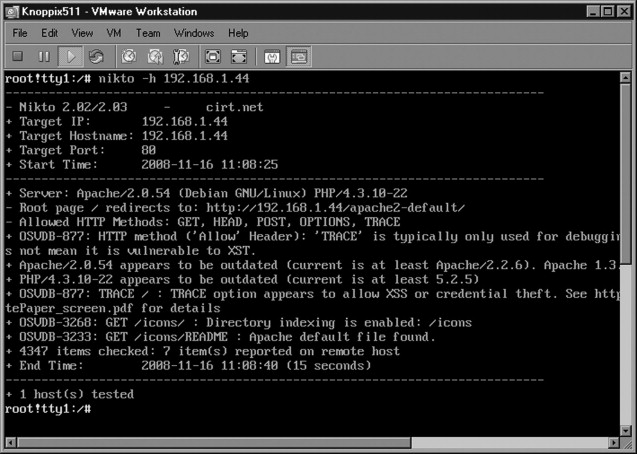
***8. Gobuster:***

*Gobuster is a directory and file brute-forcing tool designed for web application testing. Security professionals leverage it to discover hidden files and directories on web servers by systematically trying different paths and filenames. Gobuster aids in uncovering potential information leaks and security weaknesses.*

**

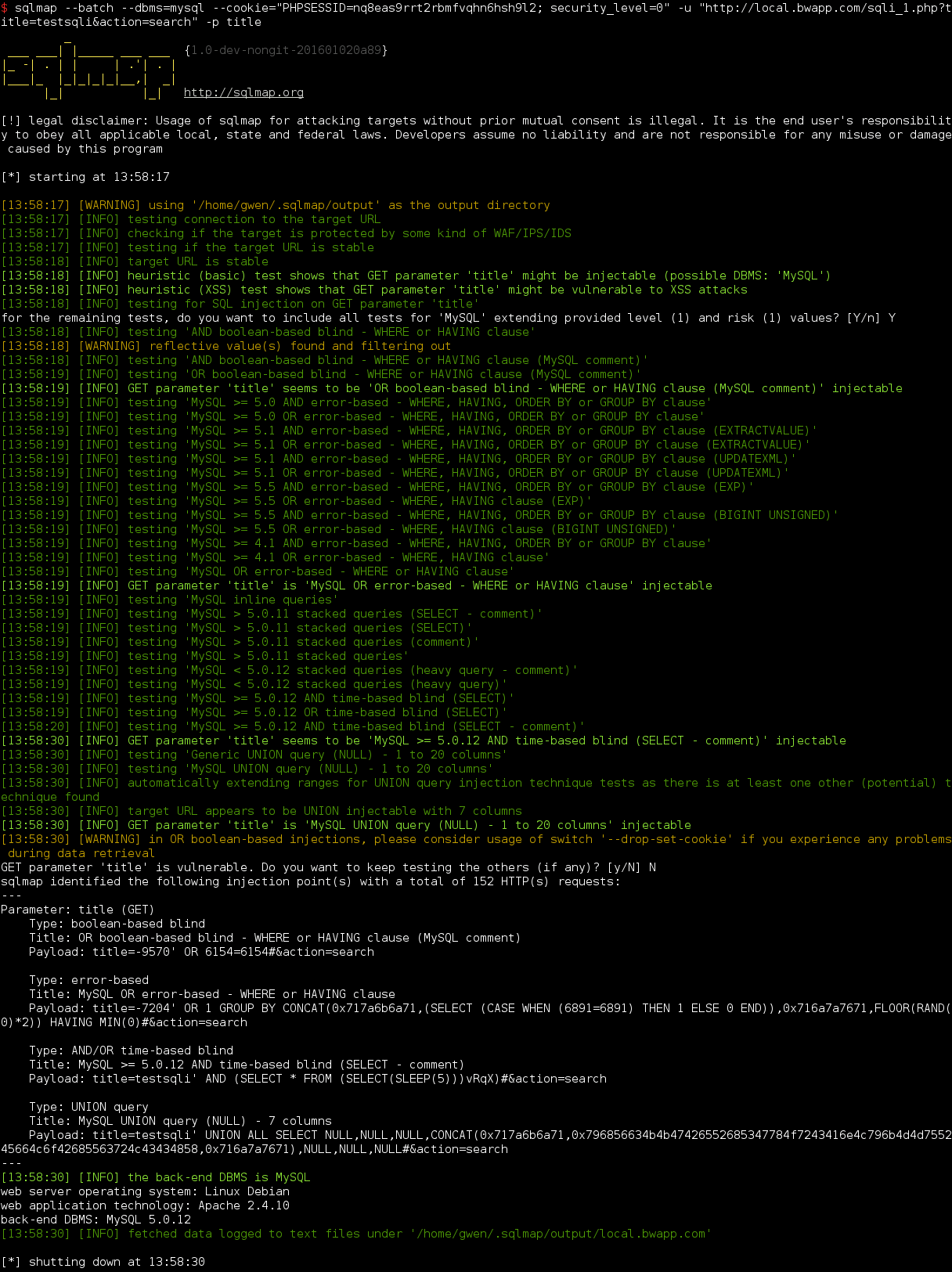
***9. Nikto:***

*Nikto is a web server vulnerability scanner that specializes in identifying security issues in web applications and servers. It scans for known vulnerabilities, misconfigurations, and common security flaws, providing security teams with valuable insights into potential risks. Nikto is an essential tool for maintaining robust web application security.*

**

***10. SQLMap:***

*SQLMap is an automated SQL injection testing tool used to detect and exploit SQL injection vulnerabilities in web applications. Security professionals rely on SQLMap to automate the identification of SQL injection flaws, enabling them to assess database security comprehensively. It aids in finding and addressing critical vulnerabilities that could compromise data integrity and confidentiality.*

**