LAB (8): Reconnaissance and Scanning

Hamzah Al-Alami (32015334503)

Ayham Al-Hindi (31915179075)

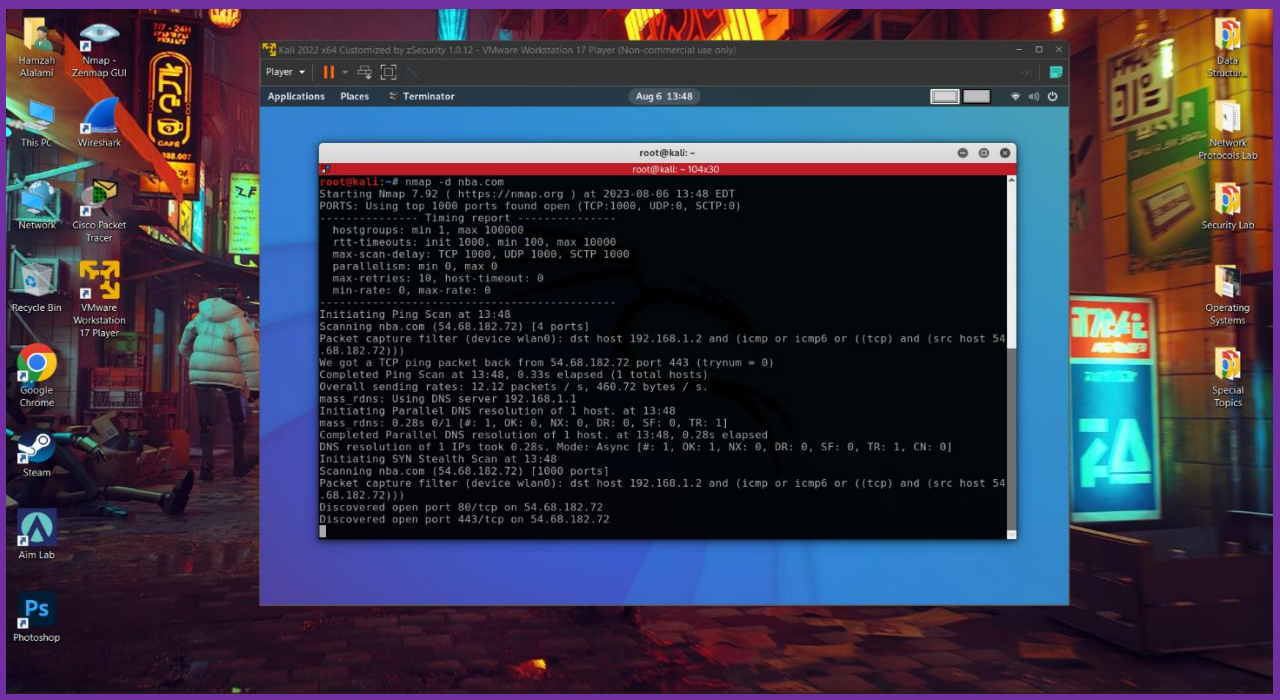
Taha Hadib (31915179032)

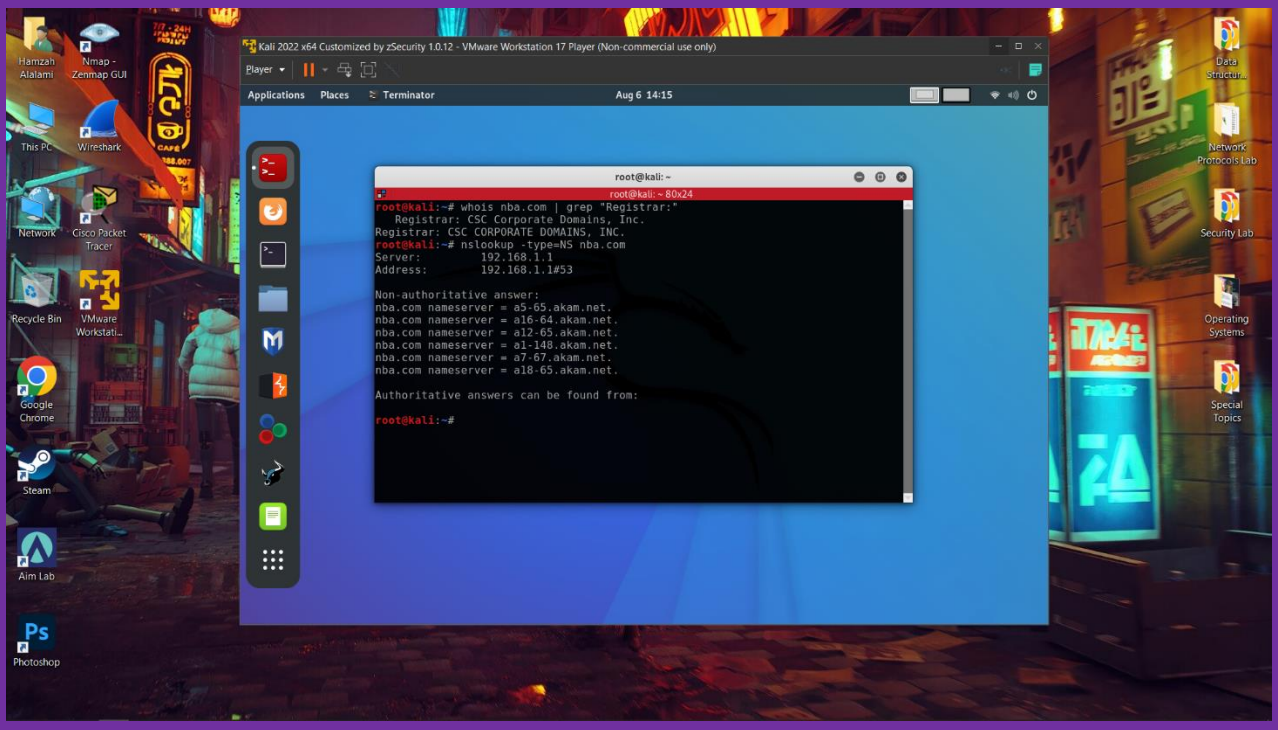
Date: 6/8/2023 (Summer Semester)

Objective: learn spying and scanning methods used to protect computer systems. exploring various ways to gather information and find weaknesses in computer systems.

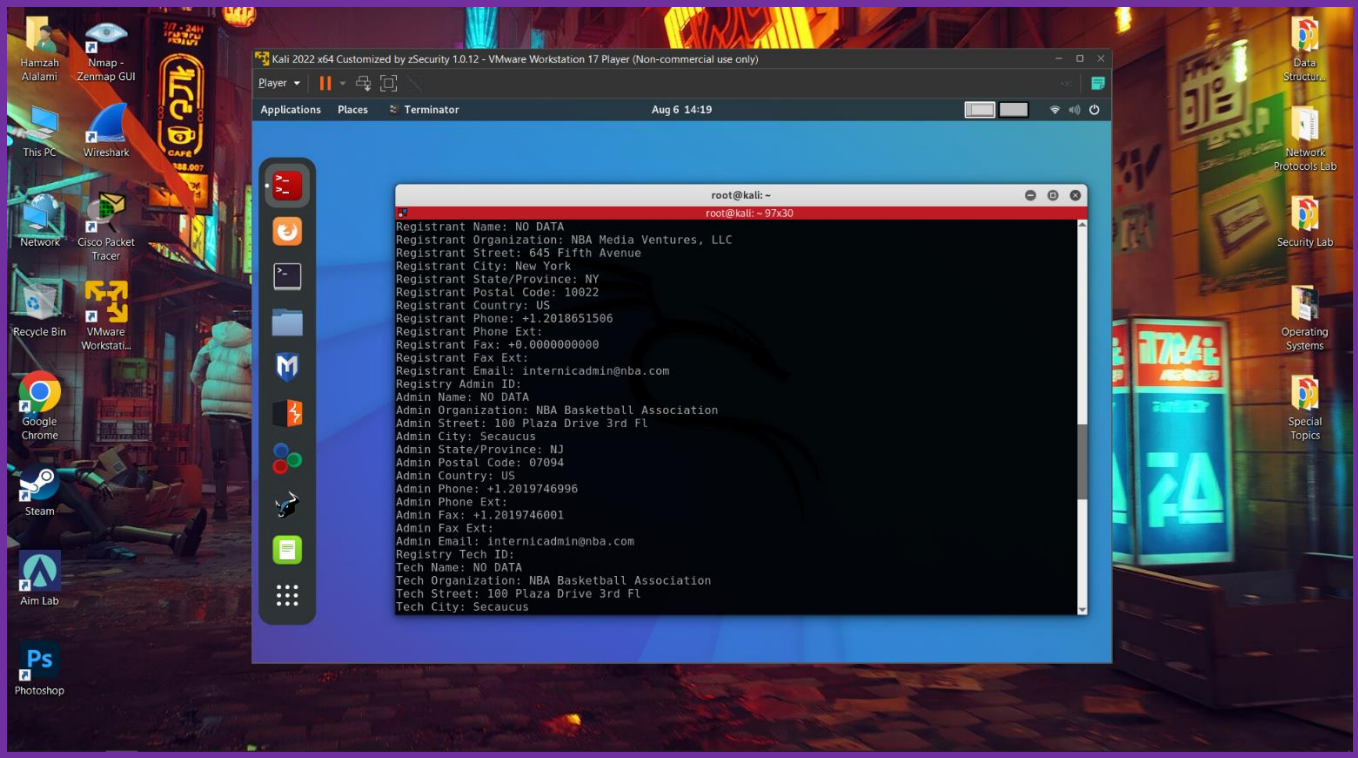
Question (1) asked us to gather info about the domain's registrar name and provide the list of authoritative DNS name servers from nba.com

we used N-map in Linux to gather this info using these commands.



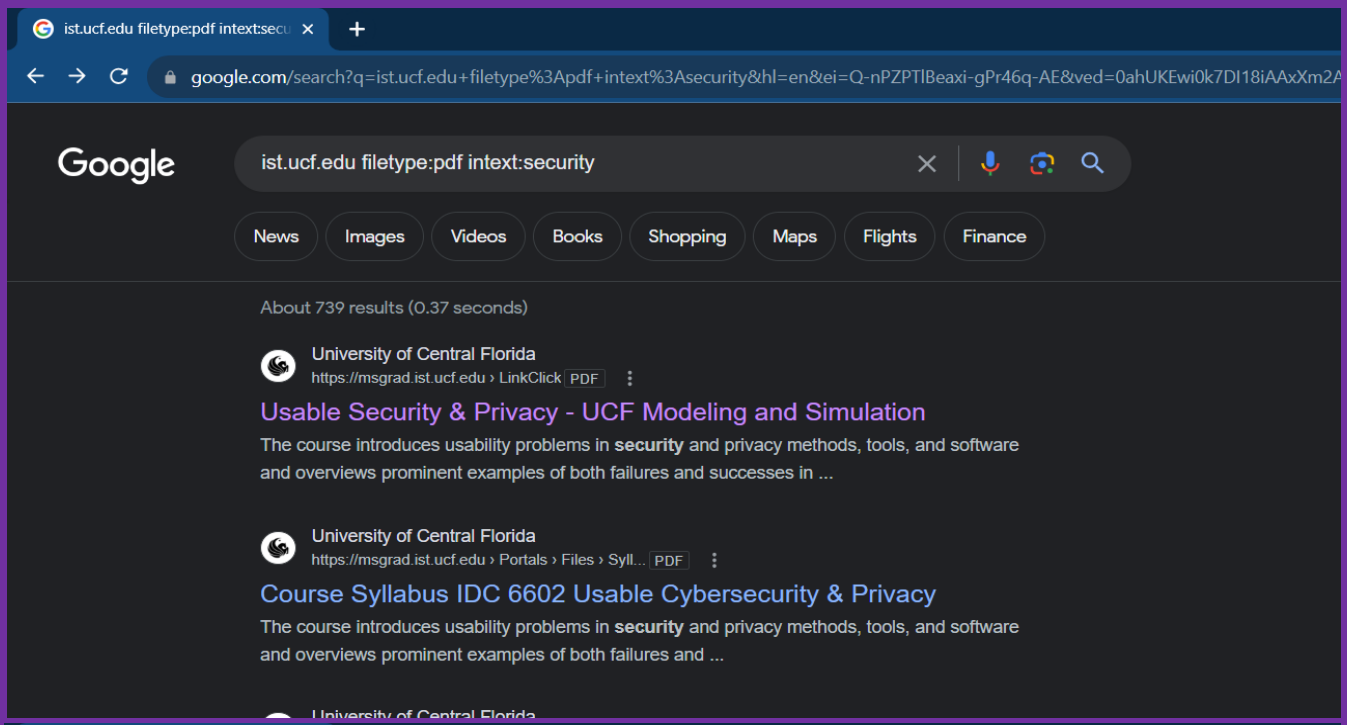


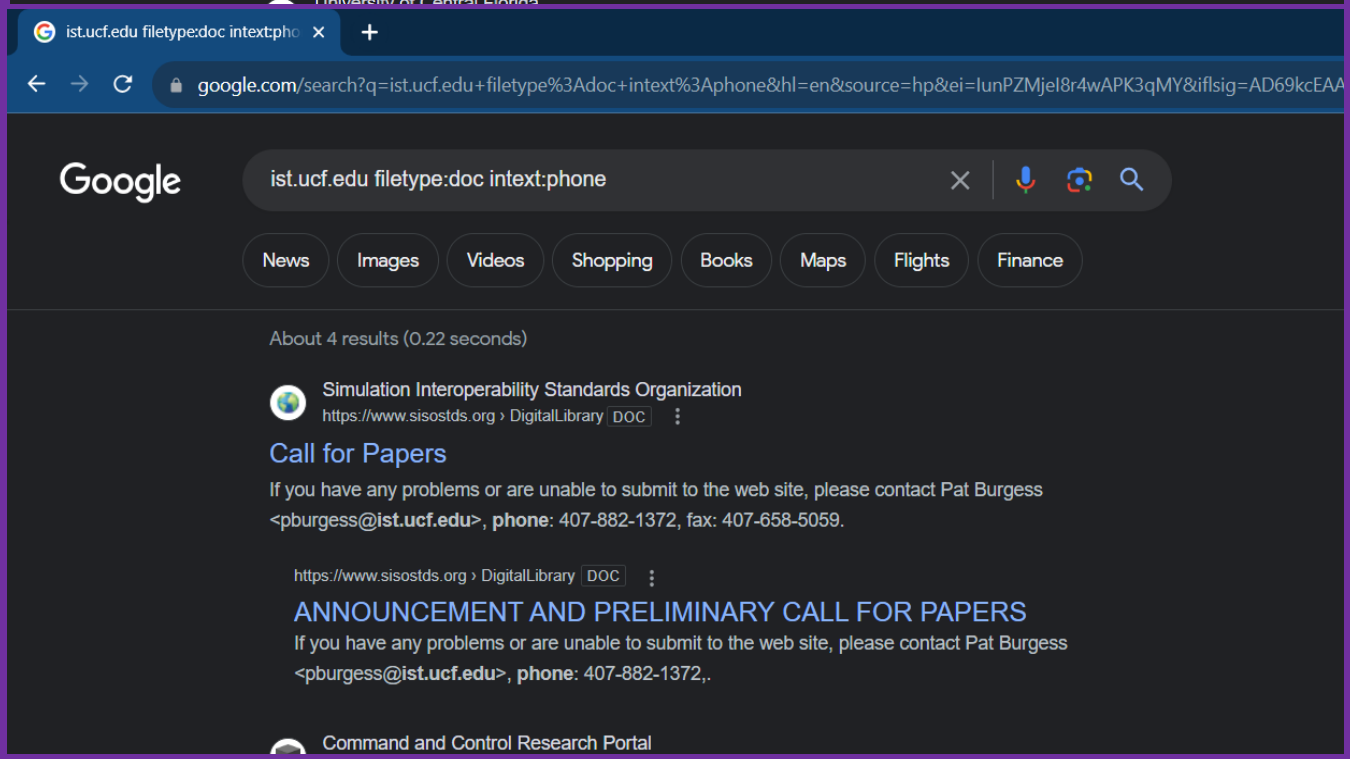
It also asked us to the domain’s admin name and, address and phone number, we gathered them using WHOIS lookup, which is a protocol that provides information about domain registration, including administrative contact details.



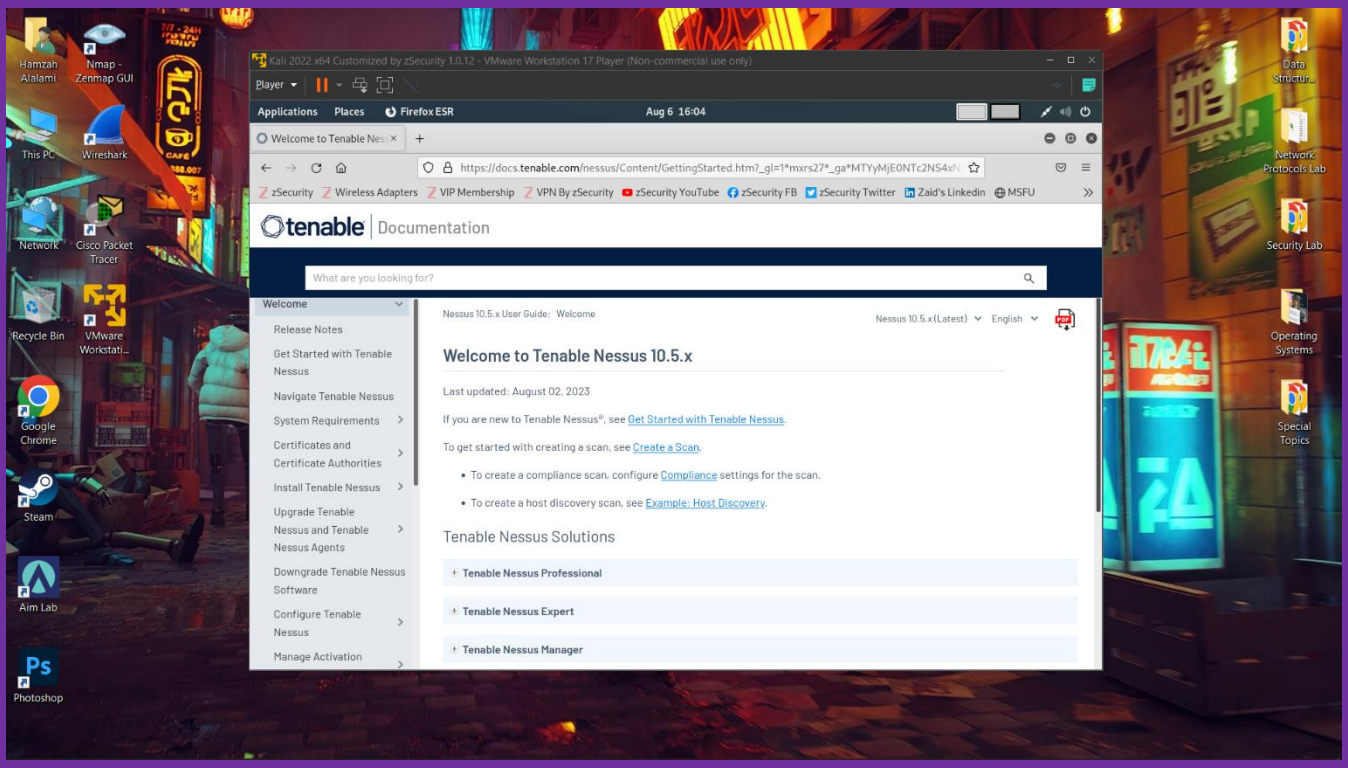
Meanwhile in Q2, it asked us to use google hacking techniques to o do information gathering about the domain “ist.ucf.edu”, list of word files that contain keyword “phone” and Find the PDF files in IST that contains “security”.

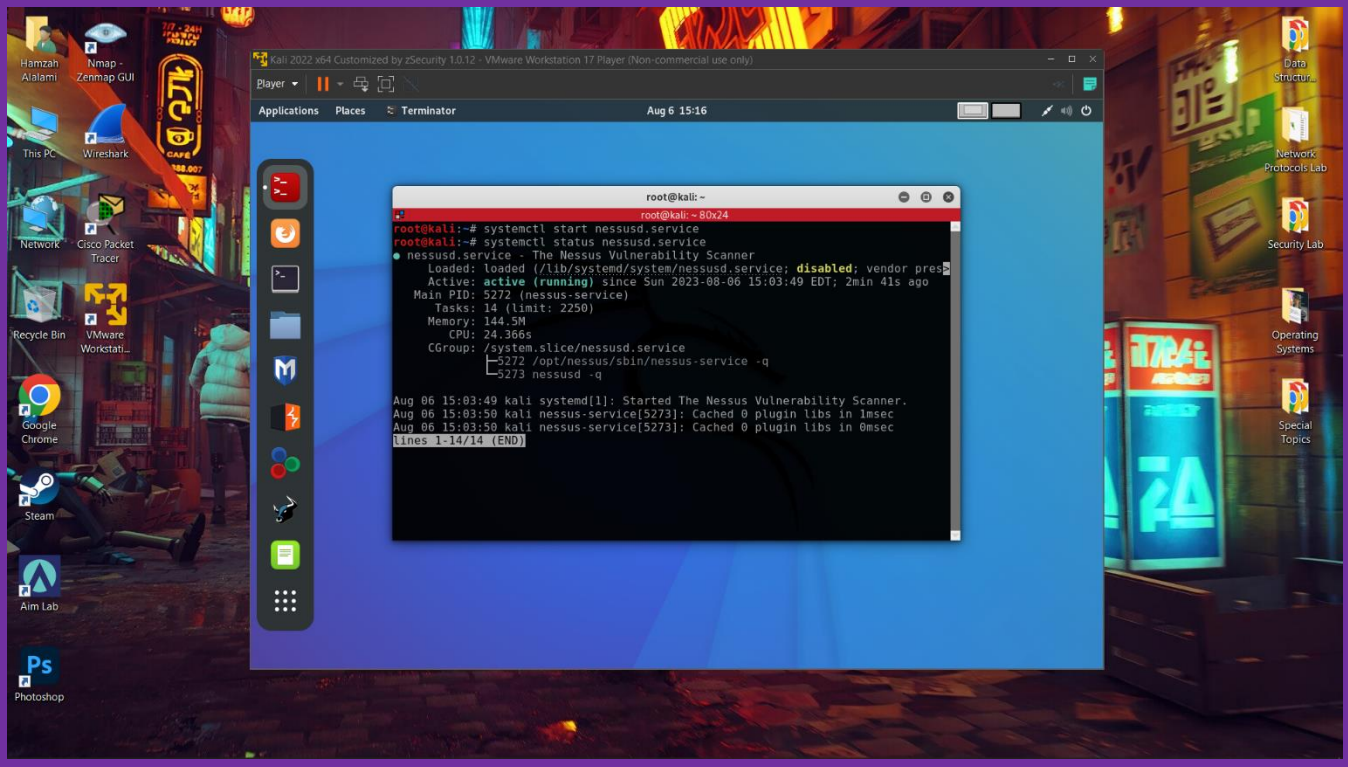
Here are the search phrases that we used to do that:



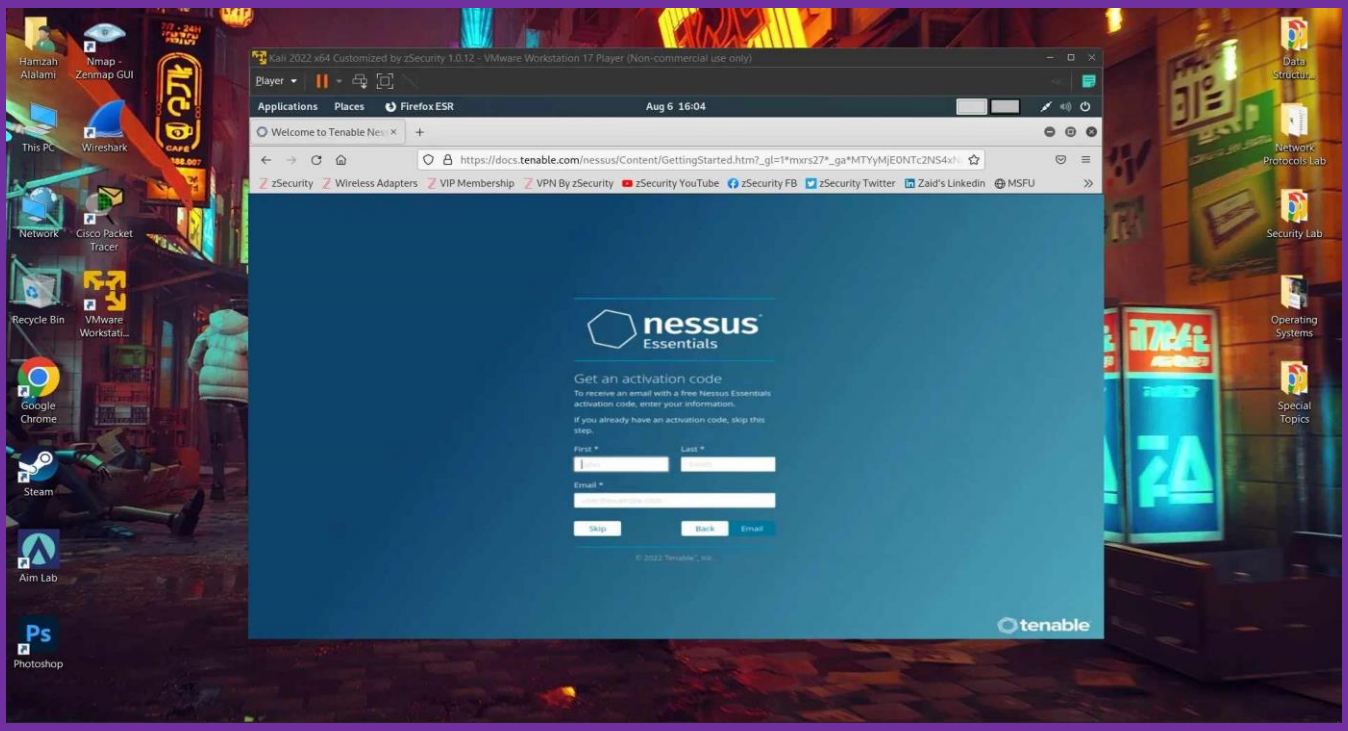


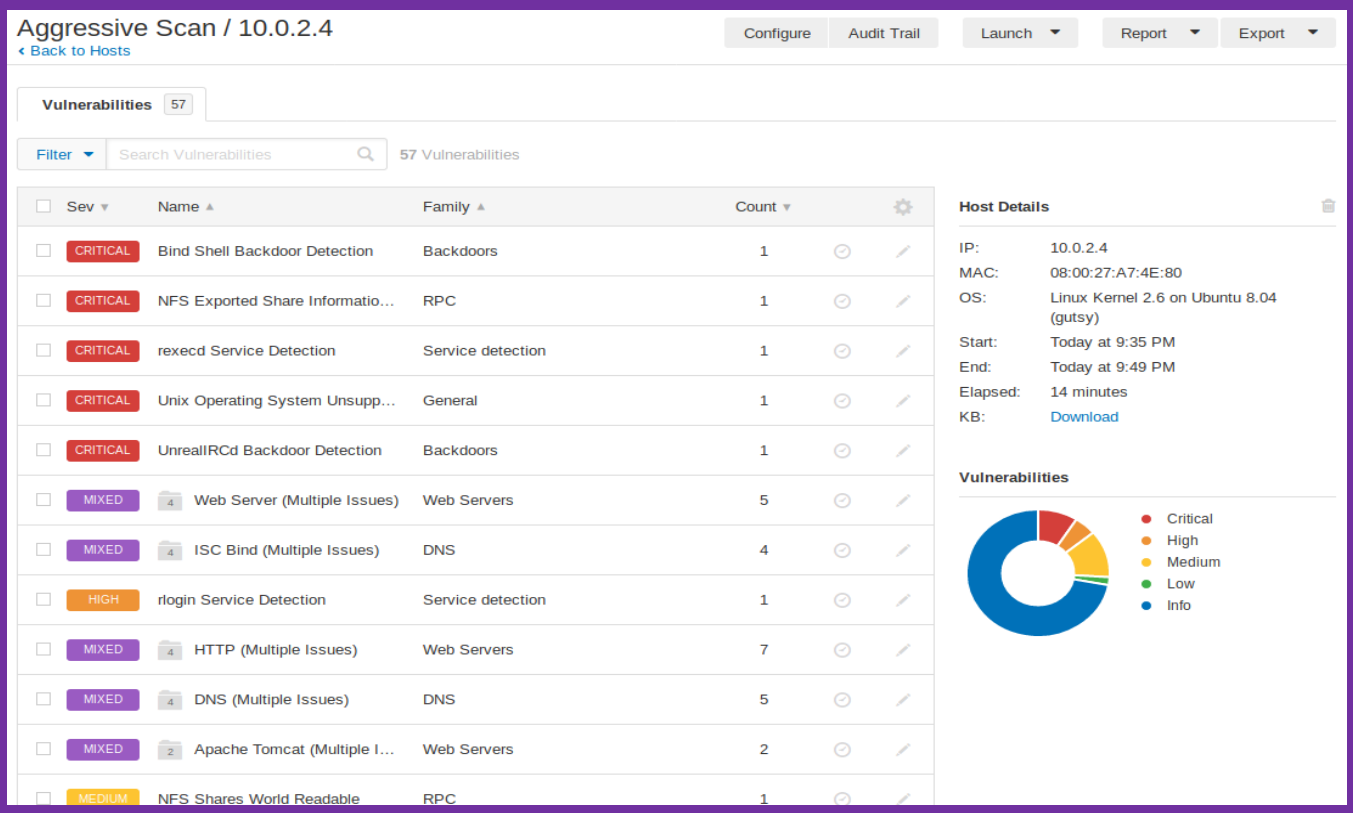
Q3 was about downloading and installing Nessus on our system and to show the Nessus login interface, then to run network scan to scan our Metasploitable Linux VM.



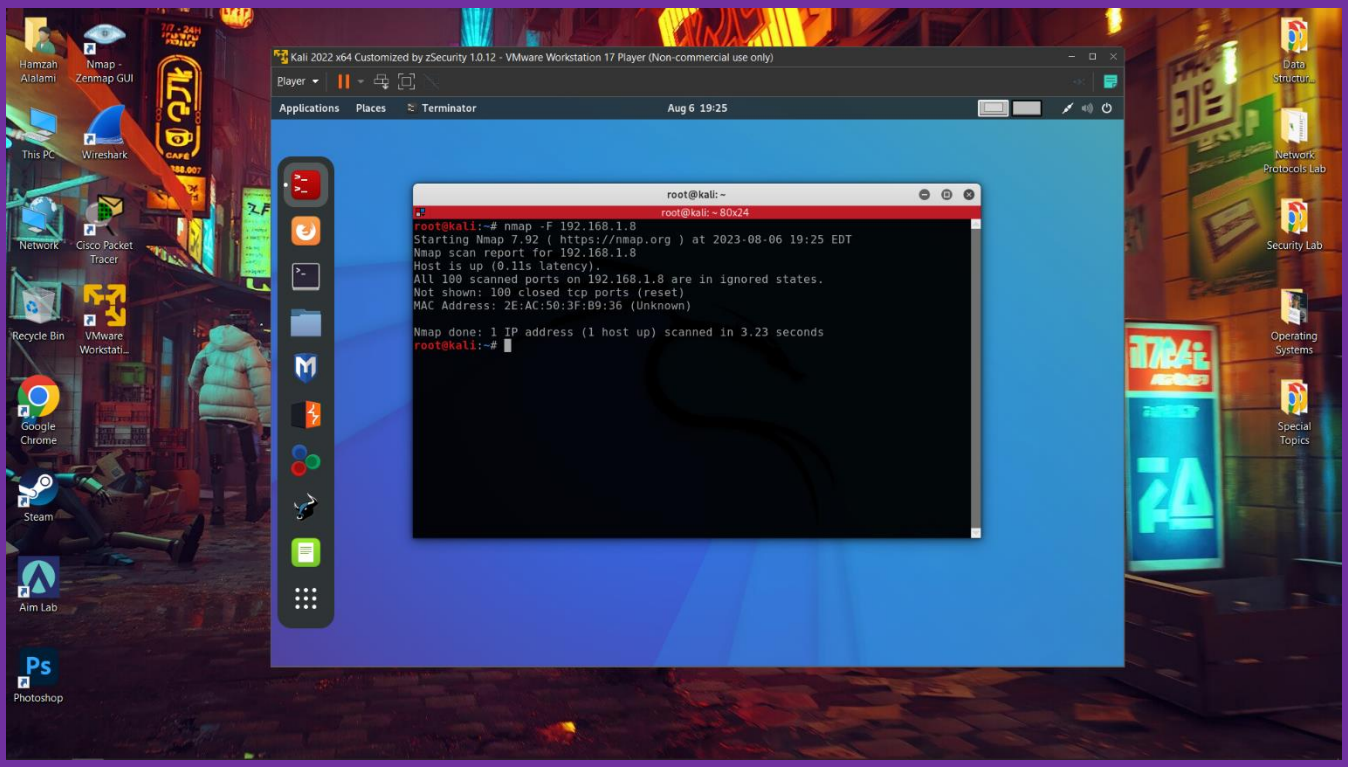


According to the report, it would be OK if we found less than 10 critical vulnerabilities, which we did.





Finally, in Q4, we were asked to conduct standard fast scan to scan our Metasploitable Linux VM. In order to discover standard service opened on the Metasploitable Linux VM.



Abstract

we explored various cybersecurity techniques such as internet information gathering, Google hacking, Nessus vulnerability scanning, and Nmap scanning. The practical exercises helped us to discover domain registrar details, find files with specific keywords, perform network scans, and identify open services.