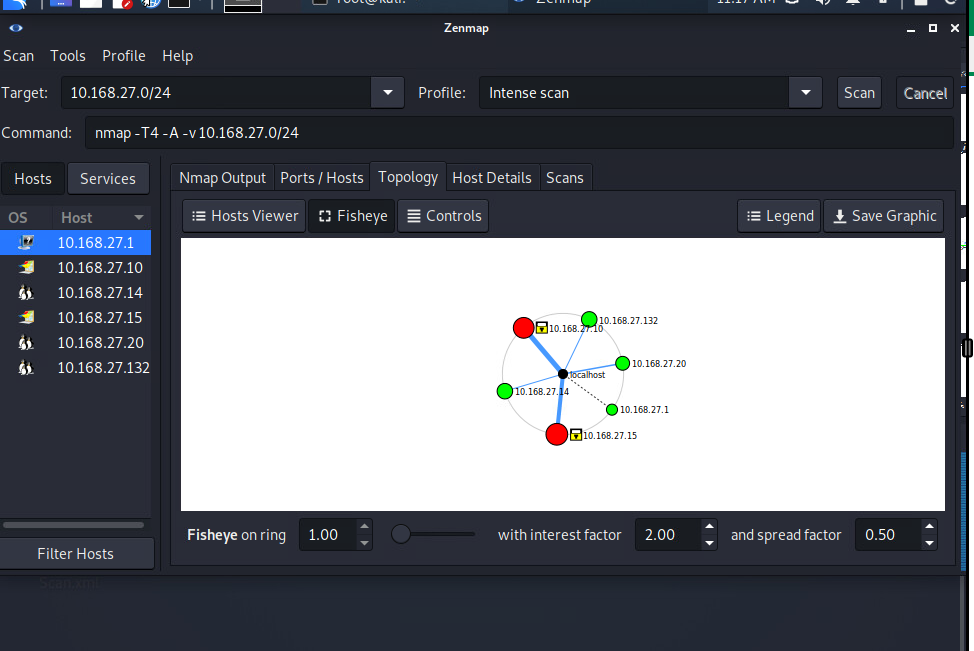
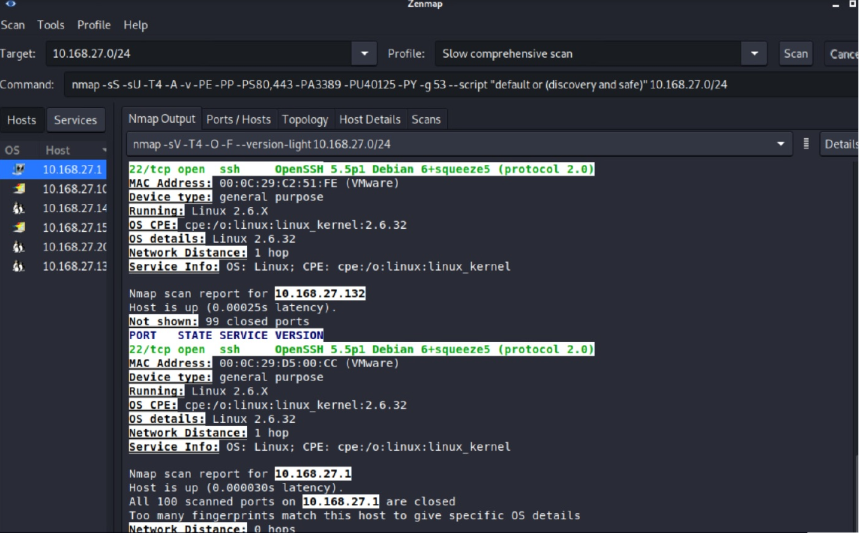
Emerging technologies in cybersecurity

# A: Network Topology Analysis

Using Zenmap, the network topology was discovered and was shown to be in the Star topology, which was composed of 6 network hosts that belong in the Star topology. Only two devices run on Windows operating systems, 10.168.27.10 and 10.168.27.15. On the other hand, 10.168.27.14, 10.168.27.20, and 10.168.27.132 belong in the Linux OS category with the impossible task of handling the OS. Devices are interconnected to both a central hub or switch in a star topology making it easy to integrate peripheral devices to the network and to enhance centralized network management. This configuration is beneficial as it gives isolated device impact and improves network efficiency by data collisions. The downside of such a setup is the potential for a single point of failure as it would result in all connected devices being affected and infrastructure costs being reduced if the central switch is not working properly. Nevertheless, this could lead to a single point of failure if the central switch fails, thereby, affecting all the connected devices and increasing infrastructure costs.



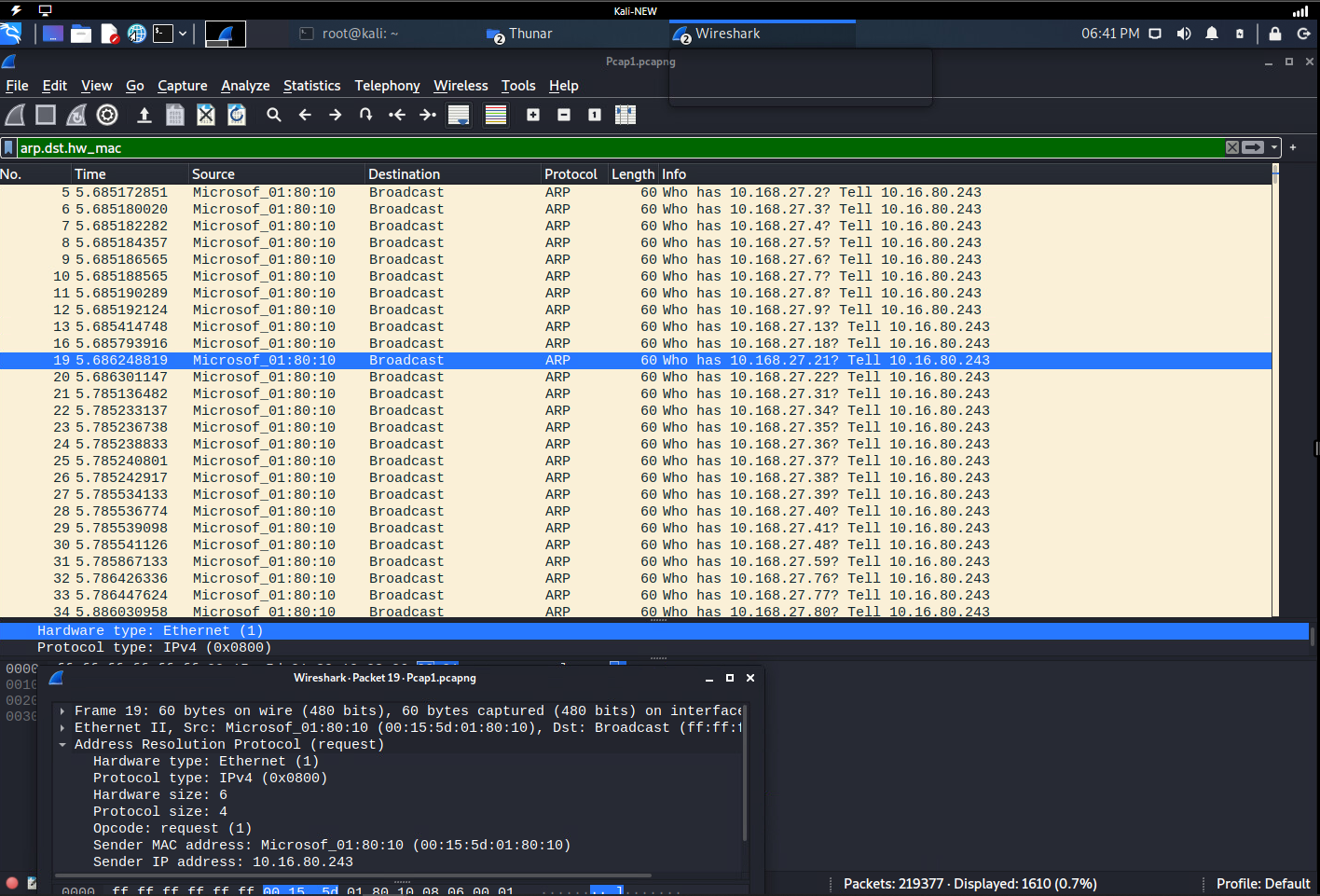


# B: Network Vulnerabilities

The Nmap scan has reflected the vulnerabilities present within the network. Particularly, 10.168.27.15 (running Windows 8.1) has port 21 dedicated to FTP that is open on the computer. Through FTP, which lacks encryption, unauthorized parties can intercept the data, thus increasing the chance of man-in-the-middle attacks and malware infiltration. Consequently, this vulnerability allows attackers to insert malicious code into FTP applications that could lead to data loss and misuse of credentials. Moreover, the hosts that contain Linux kernel 2.6.32 (10.168.27.14, 10.168.27.20, 10.168.27.132) are affected by CVE-2023-32254, a vital error in the ksmbd module that could be exploited thanks to inappropriate protected SMB2\_TREE\_DISCONNECT operations. In addition to this, the out-of-date operating systems such as Windows 2012 (10.168.27.10) and Windows 8.1 (10.168.27.15) are no longer supported by Microsoft and will remain exposed to known exploits and zero-day attacks.

# C: Wireshark Anomalies

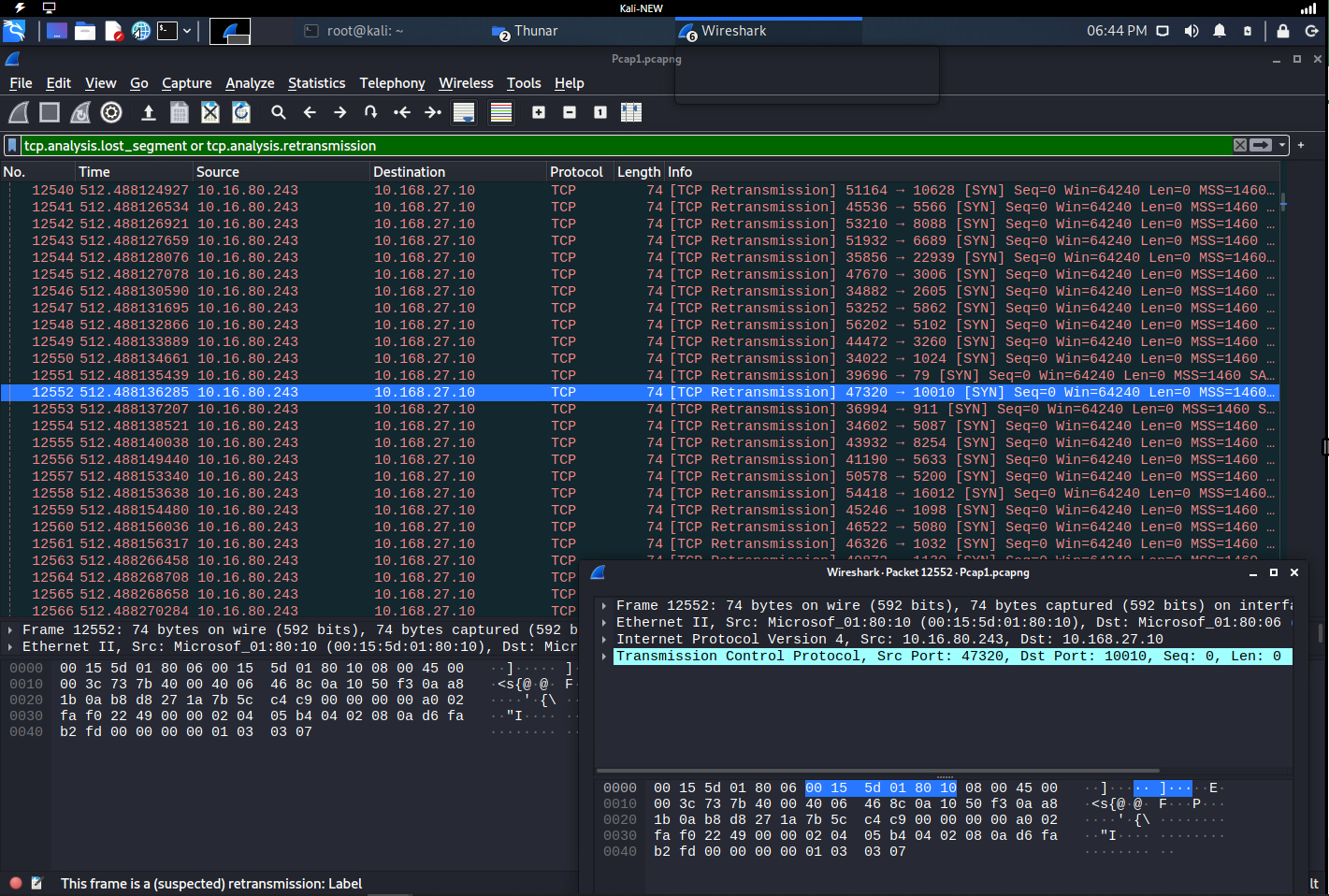
The analysis by Wireshark uncovers the fact that some activities are being carried out by malicious hackers that are suspicious steps for potential hacks on the network. To start with, a series of so-called ARP Scans sent from 10.16.80.243 are the activities of reconnaissance meant for the identification of active ones on the particular network, quite likely this is the preliminary phase of a future ARP poisoning attack. Also, the examination of the TCP packets shows quite a number of Retransmissions from the same IP address which may mean that the network is experiencing serious issues, or the IP has probably been subject to a denial-of-service (DoS) attack. On top of this, ICMP-based UDP scanning by the same IP is the first glimpse we see of a network probing activity which consists of trying to find out what are the open or closed UDP ports by sending UDP Port scanning packets.



# 

# D: Implications of Anomalies

A few actions associated with IP 10.16.80.243 come up as an explicitly organized probe with its functional objective to map the terrain and possibly reveal the weakest links in a network. An IP address revelation, thanks to ARP poisoning, which is the result of ARP scanning, allows hackers to come in between the throes of the data traffic, hence the compromise of data integrity and confidentiality. The packet retransmissions and the UDP port scanning activities propose that the network is vulnerable and it can be damaged through unauthorized access or the use of other disruptive techniques that pose a serious threat to the quietness of the network and the continuous system operation by it.



# E: Security Solutions

The unavoidable FTP vulnerability issues can be resolved by using AES (Advanced Encryption Standard) and SHA-2 (Secure Hash Algorithm). It would be a good idea to disable the use of regular FTP to work with safer FTPS, SFTP, and SSH, and so to overcome the weak points of the option of data leaking. On the part of enabling the blacklisting and whitelisting of IP addresses, only the authorized IPs can be the ones to gain admittance to the network, and by so doing, the security level is significantly improved, more so, the regular modification of the passwords makes sure that no password should be added to the list again thus ensuring that no security breaches should be there. The important point that cybersecurity advisors have made is securing the systems with the consent of the organizations to do the best we can for protection from the well-known attacks and the ones that are unknown and that are in abundance. To prevent potential intrusions by port scans and network mapping, it is necessary to scrutinize frequently a network by using tools like Nmap, Nessus, or OpenVAS. Shielding from potential threats through the port scanning process helps you to achieve a better defense mechanism, which is the unification of the network with the needs and the adopted security measures.

# F: Sources

10 Essential Tips for Securing FTP and SFTP Servers. Retrieved from [<https://www.fortra.com/blog/10-essential-tips-securing-ftp-and-sftp-servers>]

CVE Details (2023). CVE-2023-32254. Retrieved from [<https://nvd.nist.gov/vuln/detail/CVE-2023-32254>]

CISA. Understanding Patches and Software Updates. Retrieved from [<https://www.cisa.gov/news-events/news/understanding-patches-and-software-updates>]

Sectools. Vulnerability Scanners - Sectools Top Network Security Tools. Retrieved from [<https://sectools.org/tag/vuln-scanners/>]