CYBER SECURITY INTERNSHIP

Task:01 Cybersecurity Risk Assessment

MARCH 8, 2024

INTERN CAREER

Cybersecurity Risk Assessment:

Cybersecurity risk assessment is the process of identifying, evaluating, and prioritizing potential threats and vulnerabilities that could compromise the confidentiality, integrity, and availability of information systems.

Key Components of Cybersecurity Risk Assessment:

1. **Asset Identification:** Identify and prioritize assets critical to the organization, including hardware, software, data, and personnel.
2. **Threat Identification:** Identify potential threats that could exploit vulnerabilities and impact the security of assets.
3. **Vulnerability Assessment:** Assess weaknesses and vulnerabilities in systems, applications, and processes that could be exploited by threats.
4. **Risk Analysis:** Evaluate the likelihood and impact of identified risks to determine their overall risk level.
5. **Risk Mitigation:** Develop strategies to mitigate or control identified risks, including implementing security controls and best practices.

Threat Identification:

Sample Network/ System Setup:

The provided system is a small business network with a web server, database server, and multiple client workstations. The web server hosts a customer portal and the database server stores sensitive customer information.

Identify Threats and vulnerabilities:

Threats:

1. **Malware:** potential for malware infections due to web server exposure.
2. **Unauthorized Access:** Weaknesses in authentication may lead to unauthorized access.
3. **DDOS Attacks:** The web server is susceptible to Distributed Denial of Service attacks.

Vulnerabilities:

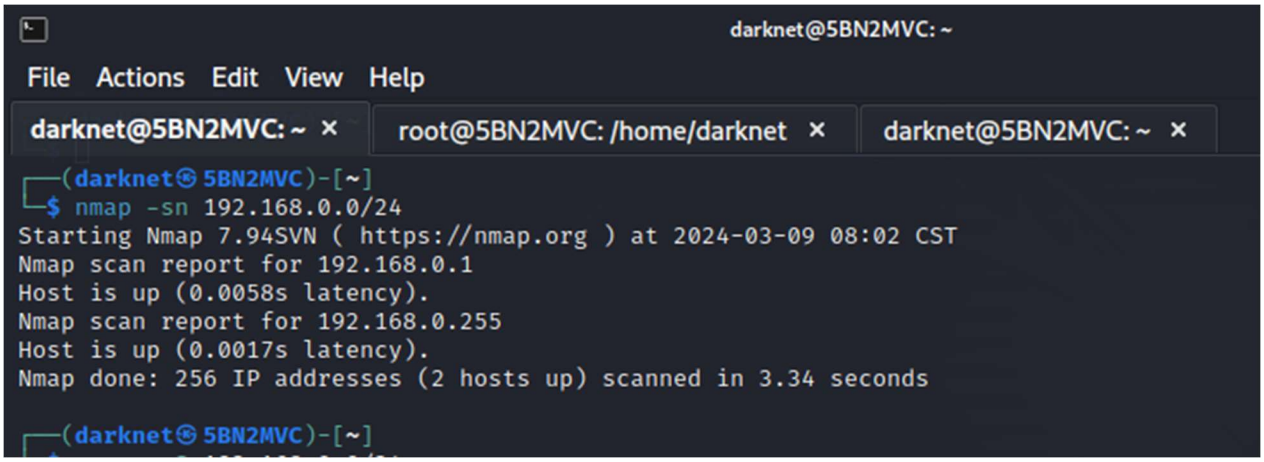
1. **Outdated Software:** The web server software may not be up to date.
2. **Weak Passwords:** Workstations might have weak passwords, increasing the risk of unauthorized access.

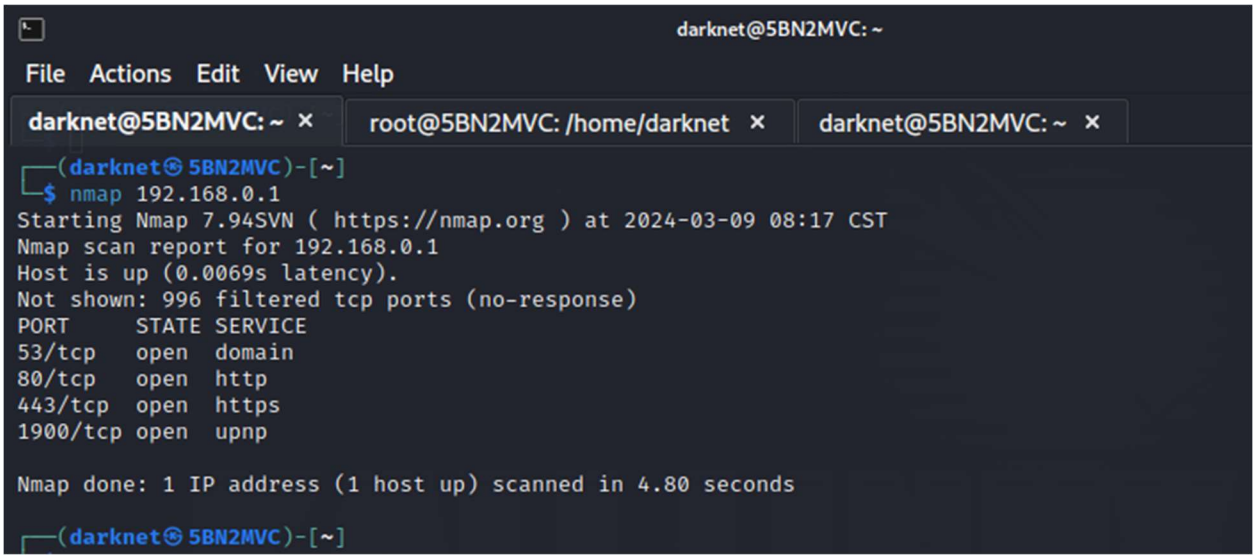
Tools for Cybersecurity Risk Assessment:

Nmap:

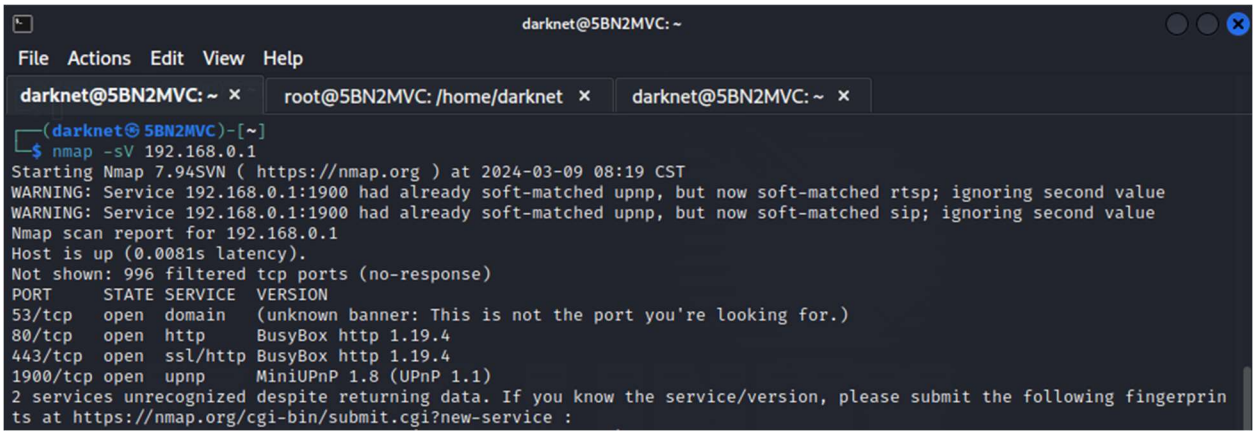
1. Conducted a network scan to identify active hosts and open ports.
2. Identified the IP addresses of the web server, database server, and workstations.

Ping Scan: The simplest way to check active hosts and open ports is by a ping scan.





Service and version detection: To identify services running on open ports and their versions.

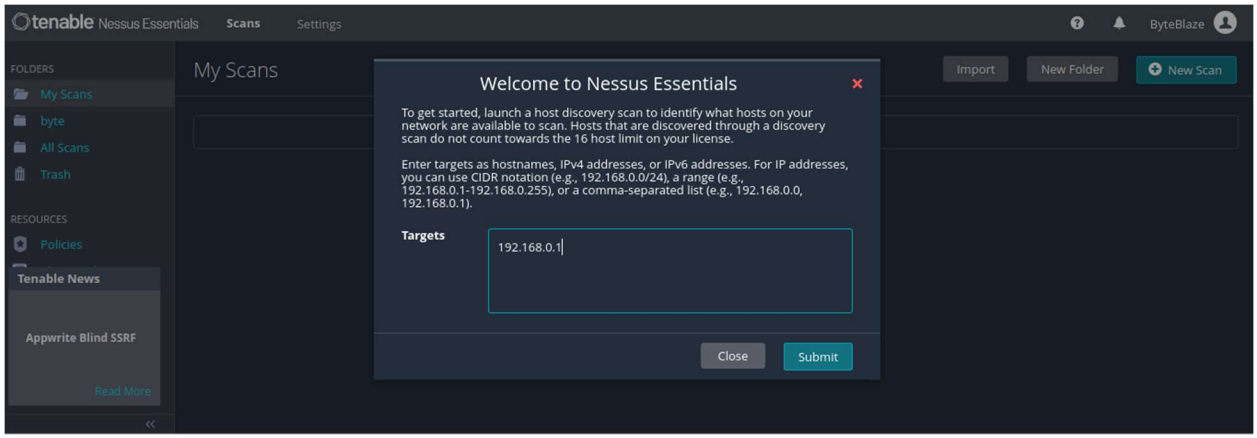


Nessus:

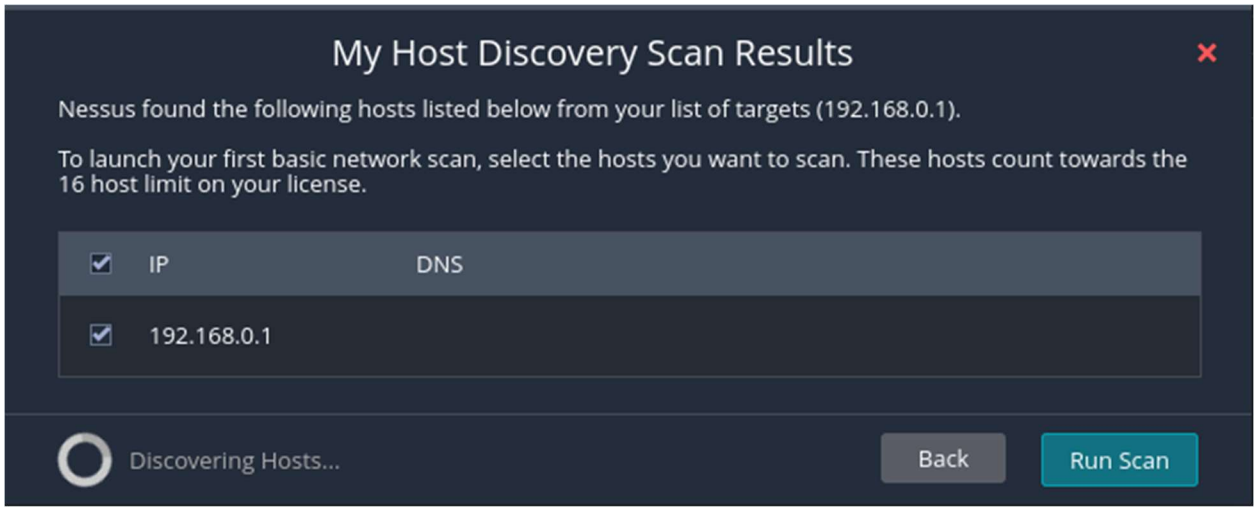
1. Performed a vulnerability scan on each identified host.
2. Discovered vulnerabilities such as outdated software versions and weak configurations.

An effective tool for vulnerability scanning and assessments, Nessus identifies security issues in systems and applications.

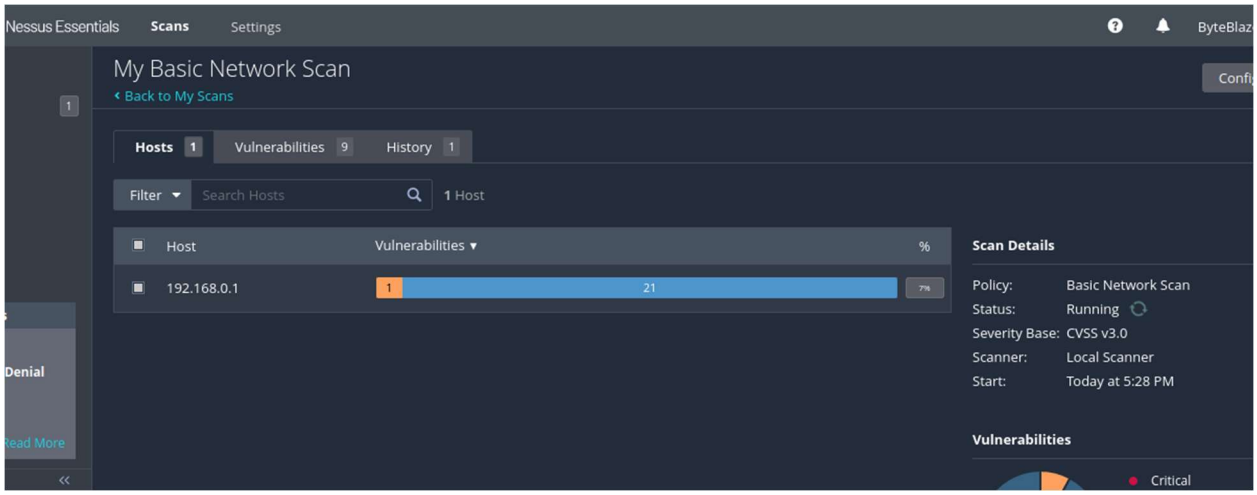
Scan targets IP:



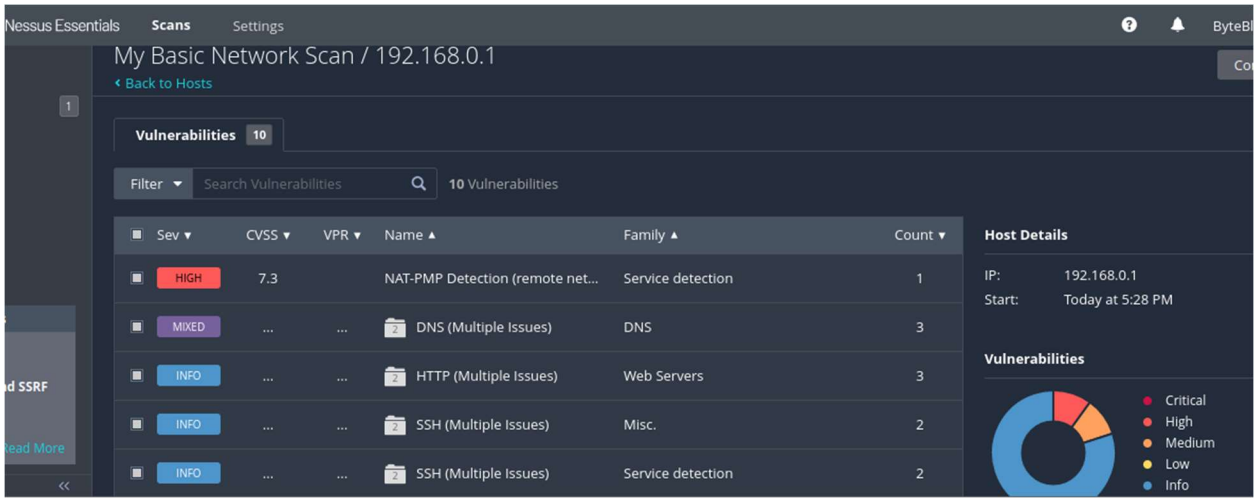
Network scan

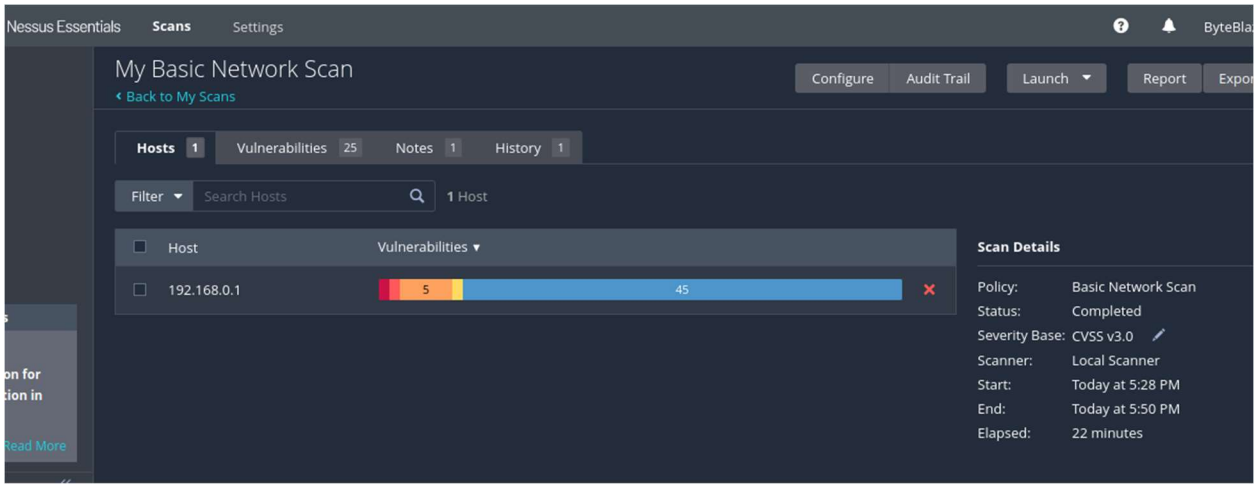


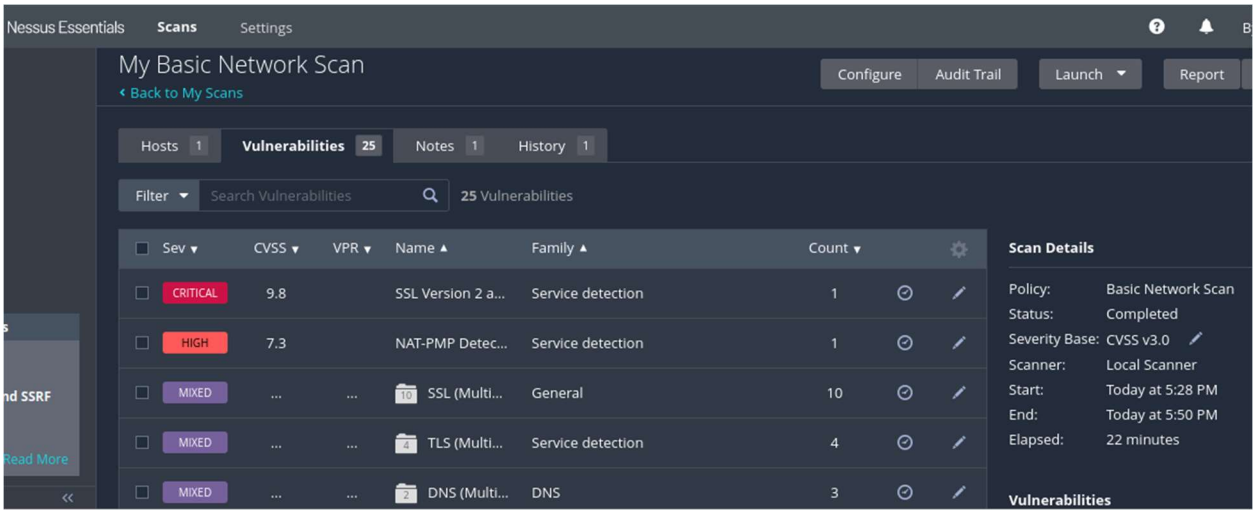
Scan Vulnerabilities



Vulnerabilities scan finds high risk



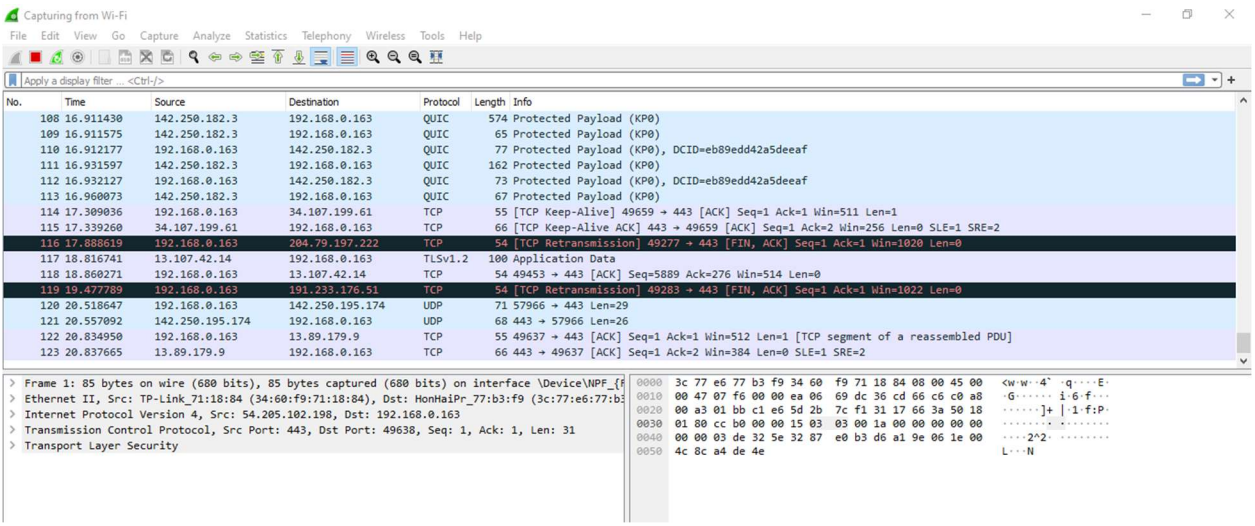


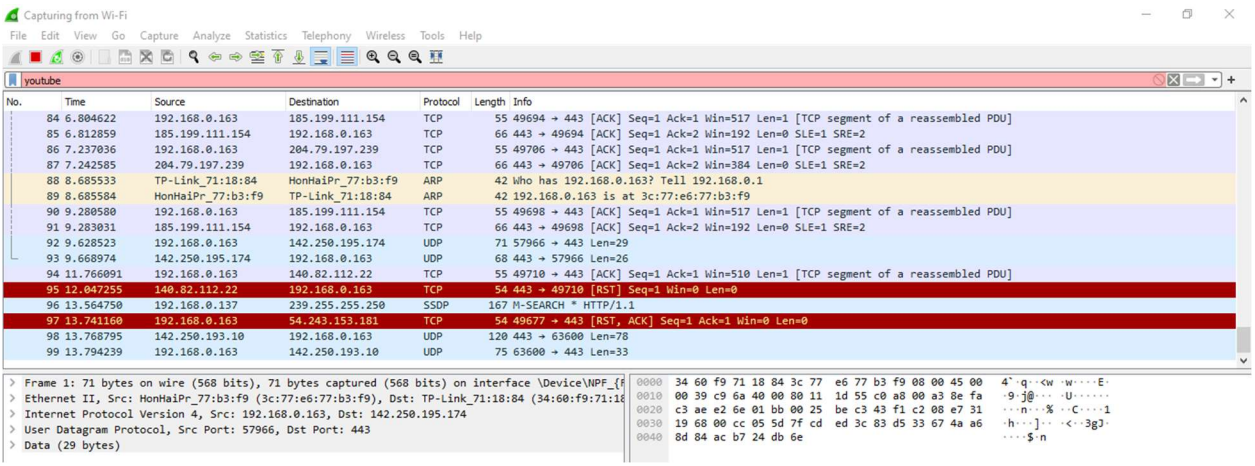


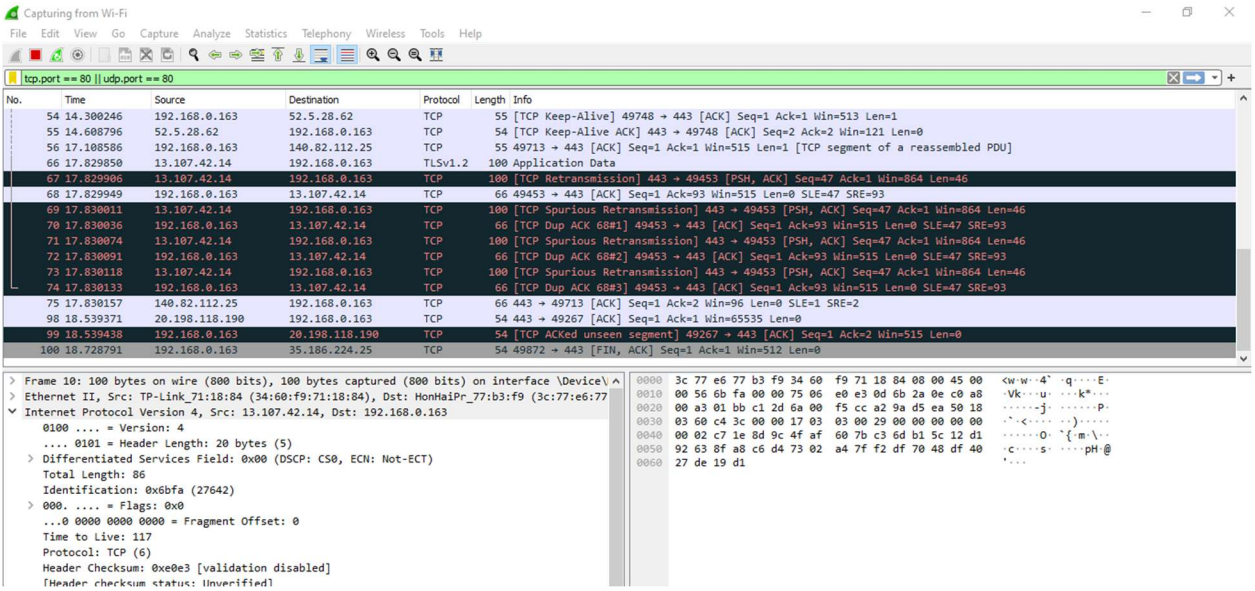
Wireshark:

Useful for network protocol analysis and troubleshooting, Wireshark helps examine and analyze network traffic for potential security issues.

1. Analyzed network traffic to identify any abnormal patterns or potential security issues.







Conclusion:

The cybersecurity risk assessment conducted as part of this internship has provided valuable insights into the security posture of the organization's digital infrastructure. Through a systematic approach, including threat identification, vulnerability scanning, risk analysis, and mitigation strategies, critical security risks have been identified and addressed.

Overall, this cybersecurity risk assessment internship has provided valuable hands-on experience and insights into the complexities of cybersecurity. As cybersecurity threats continue to evolve, the knowledge and skills gained during this internship will serve as a solid foundation for future endeavors in the field.