EC7020: COMPUTER AND NETWORK SECURITY
LABORATORY EXPERIMENT: 04
WIRELESS NETWORK SECURITY

Reg No: 2020/E/117 25/10/2024, from 13:30 to 16:30

AIM: Students will learn the fundamental principles of wireless networks and wireless network security by using network auditing tools.

OBJECTIVES:

- To understand the wireless networks.
- To understand the functionalities of network auditing.
- To understand the fundamentals of wireless network security.

Following are the tasks for this lab session. (30 Marks)

(Group Task)

1. select a network security audit tool that works with Wi-Fi networks. You have to do a detailed analysis of a Wi-Fi network which you have to create using a mobile hotspot.

   The report you submit must include details

   A. About the tool and its features

   - Nmap: Network Mapper

   Features:

   - **Host Discovery**: Scans and identifies devices connected to the Wi-Fi network.
   - **Port Scanning**: Reveals open ports that may represent security vulnerabilities.
   - **OS Detection**: Determines the operating systems running on connected devices.
   - **Service Version Detection**: Identifies software versions running on the network, which helps in finding outdated or vulnerable software.
   - **Scripting Engine (NSE)**: Extends functionality by allowing custom scripts to automate tasks like vulnerability detection and network auditing.

   B. Alternative tools available in the industry and reason for your selection

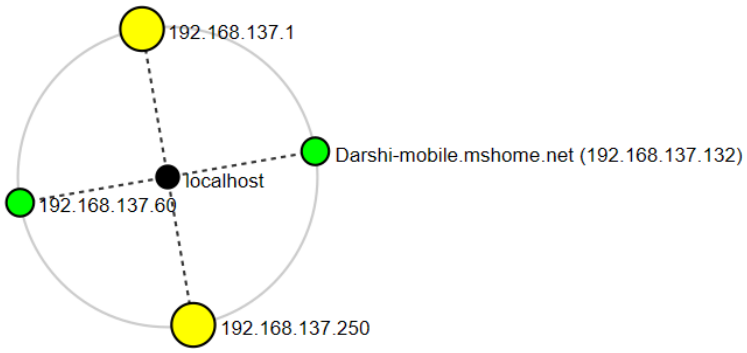
   - **Wireshark**: Packet analyzer used for monitoring traffic and troubleshooting networks.
   - **Aircrack-ng**: Suite of tools for network security assessment, focusing on Wi-Fi network penetration testing.
   - **Kismet**: Wireless network detector, packet sniffer, and intrusion detection system.
   - **NetStumbler**: Tool for detecting wireless networks, useful for signal analysis and network planning.

   - **Reason** :
     Nmap provides a comprehensive set of scanning options to gather information on various aspects of network security. Nmap works well across different devices and platforms, including the Wi-Fi network created by a mobile hotspot.It has a user-friendly command-line interface and extensive documentation, making it easy to learn and use for beginners in network security auditing.

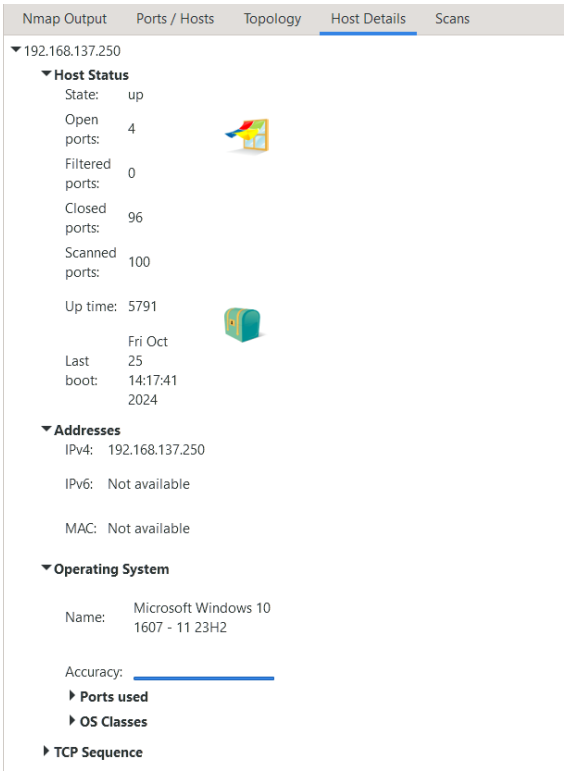
C . The Details of Wi-Fi Hotspot

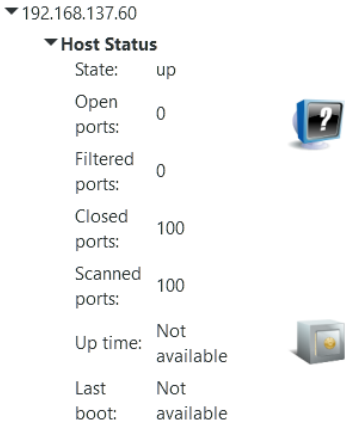
```
Windows IP Configuration


Ethernet adapter Ethernet:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . : Staff

Ethernet adapter Ethernet 2:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::511:ca33:d99d:5b99%12
   IPv4 Address. . . . . . . . . . . : 192.168.56.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :

Wireless LAN adapter Local Area Connection* 1:

   Media State . . . . . . . . . . . : Media disconnected
   Connection-specific DNS Suffix  . :

Wireless LAN adapter Wi-Fi:

   Connection-specific DNS Suffix  . : mshome.net
   Link-local IPv6 Address . . . . . : fe80::24c2:2ad2:6f74:5dcb%14
   IPv4 Address. . . . . . . . . . . : 192.168.137.250
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 192.168.137.1

Wireless LAN adapter Local Area Connection* 10:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::4584:138d:4119:f3cb%13
   IPv4 Address. . . . . . . . . . . : 192.168.137.1
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . :
```

D. Network Topology



E. Host Details





Nmap Output | Ports / Hosts | Topology | Host Details | Scans

▼ Darshi-mobile.mshome.net (192.168.137.132)

▼ **Host Status**

State:	up
Open ports:	0
Filtered ports:	0
Closed ports:	100
Scanned ports:	100
Up time:	Not available
Last boot:	Not available

▼ **Addresses**

IPv4:	192.168.137.132
IPv6:	Not available
MAC:	E2:2D:38:5B:F7:4A

▼ **Hostnames**

Name -	Darshi-mobile.mshome.net
Type:	- PTR

▶ **Comments**

▼ 192.168.137.1

▼ **Host Status**

State:	up
Open ports:	4
Filtered ports:	0
Closed ports:	96
Scanned ports:	100
Up time:	5784
Last boot:	Fri Oct 25 14:17:41 2024

▼ **Addresses**

IPv4:	192.168.137.1
IPv6:	Not available
MAC:	Not available

▼ **Operating System**

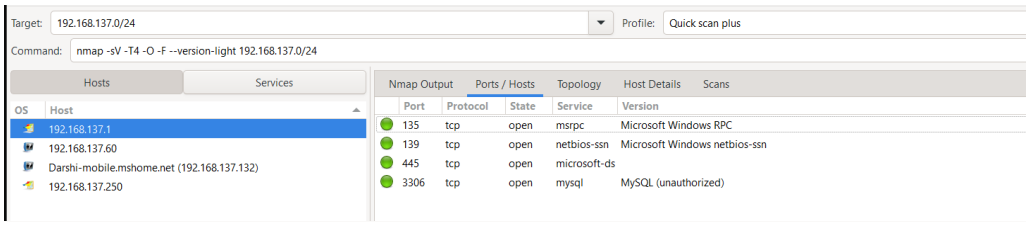
Name:	Microsoft Windows 10 1607 - 11 23H2
Accuracy:	

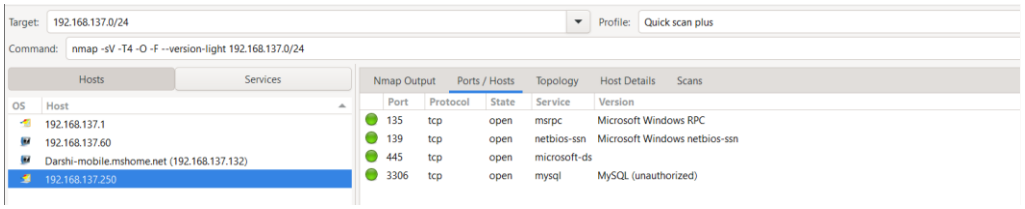
▶ **Ports used**

▶ **OS Classes**

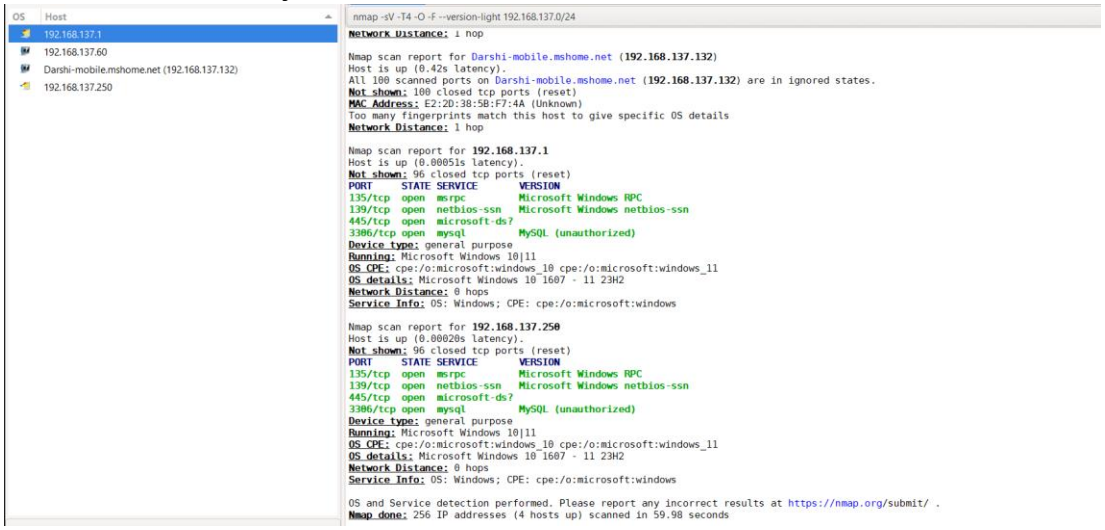
▶ **TCP Sequence**

▶ **IP ID Sequence**





F. Network Analysis



2. You have to describe the Evolution of Wireless security protocols clearly. And include comparison.

Wireless security protocols have evolved significantly over time to address vulnerabilities, improve encryption, and meet the growing demands of secure wireless communication. Each protocol was developed to solve problems of its predecessor, offering enhanced features and better resistance to attacks.

WEP (Wired Equivalent Privacy)

WEP was the first wireless security protocol introduced as part of the original IEEE 802.11 standard in the late 1990s. It aimed to provide confidentiality comparable to wired networks, but due to its weak RC4 encryption algorithm and poor key management, it quickly became outdated. WEP keys could be easily cracked due to predictable patterns in the encryption, leaving networks vulnerable to attacks.

- Encryption Algorithm: RC4, which was later found to have significant vulnerabilities.
- Key Management: Simple and weak, making WEP keys susceptible to brute-force and replay attacks.
- Resistance to Attacks: Minimal. WEP could be breached in minutes with basic cracking tools, which rendered it obsolete as Wi-Fi usage grew.

WPA (Wi-Fi Protected Access)

WPA was designed as a temporary solution to WEP's vulnerabilities. It incorporated some improvements, such as the Temporal Key Integrity Protocol (TKIP) for better encryption and key management, but still had limitations.

- Encryption Algorithm: TKIP, which improved security by dynamically generating keys for each data packet.
- Key Management: Improved over WEP, allowing per-packet key changes, which limited the scope of data available to potential attackers.
- Resistance to Attacks: More resilient than WEP but still susceptible to certain attacks, especially if a weak passphrase was used. WPA became less effective as advanced cracking techniques developed.

WPA2 (Wi-Fi Protected Access 2)

WPA2, based on the IEEE 802.11i standard, marked a major improvement in Wi-Fi security. It replaced TKIP with the more secure AES (Advanced Encryption Standard) and strengthened key management.

- Encryption Algorithm: AES, which is highly secure and still widely used today for protecting sensitive information.
- Key Management: Enhanced, providing robust encryption and regular key changes.
- Resistance to Attacks: Strong, as WPA2 AES encryption made it highly resistant to most attacks. It became the standard for Wi-Fi security in both enterprise and personal networks

WPA3 (Wi-Fi Protected Access 3)

WPA3 is the latest and most secure protocol, addressing vulnerabilities found in WPA2 and introducing new security features to combat evolving threats.

- Encryption Algorithm: Continues to use AES but includes improvements for better data protection.
- Key Management: Enhanced with a new handshake method, Simultaneous Authentication of Equals (SAE), which is more resistant to offline dictionary attacks.
- Resistance to Attacks: Offers strong defenses against brute-force attacks and includes features like individualized encryption in public networks, which protects users on open Wi-Fi from unauthorized eavesdropping.

Protocol	Security Strength	Encryption Algorithm	Key Management	Resistance to Attacks
WEP	Weak encryption	RC4	Limited	Highly vulnerable to various attacks
WPA	Improved over WEP	TKIP	Improved over WEP	Still susceptible to attacks on weak passwords
WPA2	Stronger security	AES	Enhanced	Resistant to most known attacks
WPA3	Highest current security	AES with improvements	Advanced (SAE handshake)	Strongest resistance to offline attacks and more

3. Compare the difference between Wired LAN and Wireless Network security protocols.

- In a wired LAN, physical access is required to connect to the network. This limited accessibility makes wired networks inherently more secure, as unauthorized users cannot access the network without a physical connection. By contrast, a wireless network transmits data through radio signals, which can extend beyond the physical boundaries of a building. This makes wireless networks more accessible to unauthorized users, requiring additional security measures to protect against potential intruders.
- Both networks use encryption, though wireless networks demand stronger protocols due to their vulnerability. Wired networks typically rely on WPA2 encryption when encryption is required, but wireless networks often use WPA2 or WPA3 encryption, with WPA3 being more secure. WPA3 protects data traffic by using a more robust encryption method, which guards against decryption attacks even if some packets are intercepted.
- Both wired and wireless networks often use the 802.1X protocol for authentication, which acts as a gatekeeper to prevent unauthorized access. However, wireless networks benefit more from this type of security protocol because they are more accessible to unauthorized users. In wireless networks, 802.1X is often used alongside WPA2 Enterprise to enforce strong authentication, making it harder for attackers to access the network.
- Wired networks can use VLANs (Virtual Local Area Networks) to segment parts of the network, separating sensitive data or groups of devices for improved security. Wireless networks also employ network segmentation but might use multiple SSIDs (network names) to separate user groups, like guests and employees, which can enhance security by controlling access.
- Wireless networks implement added security policies to protect the transmission over the air. This includes MAC address filtering, which allows only pre-approved devices to connect, and SSID hiding, where the network’s name is hidden from public view to reduce visibility to unauthorized users.

4. Briefly describe about packet tracing. And explain how packet tracer helps to crack Wi-Fi passwords.

Packet tracing is the process of capturing and examining data packets that travel over a network. This technique is widely used for network troubleshooting, performance monitoring, security analysis, and protocol diagnostics.

- How Packet Tracing Works: Packet tracing involves capturing data packets as they travel between devices on a network. These packets contain valuable information, including the sender and receiver's IP addresses, the data contents, and protocol details. This information is analyzed to monitor data flows, diagnose network issues, or detect security threats. Tools like Wireshark, Tcpdump, and SolarWinds allow network administrators to capture and analyze packet data effectively.
- Applications of Packet Tracing: Packet tracing has various applications, especially in network diagnostics and security:
    - Network Troubleshooting: Network administrators use packet tracing to identify connectivity issues, bottlenecks, and latency. By analyzing packets, they can trace where communication fails and identify potential hardware or configuration problems.
    - Security Monitoring: Packet tracing helps detect unauthorized access or unusual data flows, making it a valuable tool for identifying and mitigating security breaches. For instance, unexpected IP addresses sending or receiving data can indicate a potential intrusion.
    - Protocol Analysis: Packet tracing helps analyze the behavior of different network protocols, which is crucial for ensuring compliance with standards and for understanding how different devices interact over a network.
    - Packet Tracing and Wi-Fi Security: In the context of Wi-Fi security, packet tracing can capture the handshake process between a device and a wireless network. This handshake includes an exchange of encrypted information that allows access to the network. Using specialized tools, attackers might capture and analyze this handshake in an attempt to guess the network's password. Although ethical hackers may use this method

Discussion

In this lab, the auditing tool Nmap was employed to perform an in-depth analysis of a hotspot connection. The primary objective was to connect multiple devices to the hotspot network and gather critical data, including each device's MAC and IP addresses. This study delved into the intricacies of wireless network security, a critical area given the expansion of wireless networks in both residential and commercial settings. While wireless networks offer convenience, they also expose users to potential security vulnerabilities. To counter these threats, various security protocols—such as WPA2, WPA, and WEP—have been implemented to bolster wireless network protection. This lab emphasized the importance of these protocols and highlighted the role of network auditing tools like Nmap in identifying and mitigating security issues within wireless environments.

Conclusion

Network auditing tools provide invaluable insights into the structure and security status of networks by revealing essential details about connections and devices. However, the exposure of such sensitive data poses significant security risks, as malicious actors could exploit this information. As a result, safeguarding network data from unauthorized access has become crucial. In response to these risks, various wireless security protocols have been introduced and continuously improved, although certain vulnerabilities persist. The field of wireless security remains a dynamic one, continually evolving to address new challenges and protect networks from potential exploitation.

Write your answers in this Lab Instruction sheet with the file name EC7020_L4_YourRegNo. Submit it as a PDF document archive all files and upload it to the teams. The same name conversion applies for the Zip.