port 20 (FTP Data Transfer):

1. Data Interception
2. Brute Force Attacks
3. Data Modification
4. Data Injection
5. FTP Bounce Attacks
6. Denial of Service (DoS)
7. Username Enumeration
8. Exposure of Directory Structure
9. Malware Distribution

port 21 (FTP Control):

1. Plain Text Credentials
2. Brute Force Attacks
3. Data Interception
4. FTP Bounce Attacks
5. Username Enumeration
6. Malicious Commands
7. Denial of Service (DoS)
8. Server Misconfiguration
9. Backdoor Exploitation
10. Malware Distribution

port 22 (SSH):

1. Brute Force Attacks
2. Weak Passwords
3. SSH Key Vulnerabilities
4. Protocol Vulnerabilities
5. Denial of Service (DoS)
6. Session Hijacking
7. Man-in-the-Middle Attacks
8. Shellshock and Other Vulnerabilities
9. Misconfigured Access Controls
10. Malware Distribution
11. Privilege Escalation
12. Insider Threats

port 23 (Telnet):

1. Credential Sniffing
2. Brute Force Attacks

3. Man-in-the-Middle Attacks
4. Session Hijacking
5. Command Injection
6. Data Tampering
7. Denial of Service (DoS)
8. Unencrypted Traffic
9. Default Credentials
10. Rogue Servers
11. Eavesdropping
12. Password Sniffing

port 25 (SMTP - Simple Mail Transfer Protocol):

1. Email Spoofing
2. SPAM Relay
3. Email Header Manipulation
4. Denial of Service (DoS)
5. Brute Force Attacks
6. Mail Bombing
7. Malware Distribution via Email
8. Email Content Interception
9. Directory Harvest Attacks (DHA)
10. Unauthorized Access to Mailboxes

port 53 (DNS - Domain Name System):

1. DNS Spoofing
2. DNS Cache Poisoning
3. DNS Amplification Attacks
4. DNS Hijacking
5. Zone Transfer Attacks
6. DNS Query Flood Attacks
7. DNS Tunneling
8. DDoS Attacks
9. Information Disclosure via DNS
10. Zone Enumeration

port 69 (Trivial File Transfer Protocol - TFTP):

1. TFTP Data Interception
2. Unauthorized Access to Files
3. Lack of Authentication
4. Insecure Data Transfer

5. Denial of Service (DoS)
6. Exploitation of Insecure Configurations

port 80 (HTTP - Hypertext Transfer Protocol):

1. Cross-Site Scripting (XSS)
2. SQL Injection
3. Cross-Site Request Forgery (CSRF)
4. Remote Code Execution
5. Directory Traversal
6. Insecure File Uploads
7. Server Misconfigurations
8. Information Disclosure
9. Session Hijacking
10. Brute Force Attacks
11. Denial of Service (DoS)
12. Vulnerable Web Applications

port 110 (POP3 - Post Office Protocol version 3):

1. Email Account Compromise
2. Plain Text Authentication
3. Brute Force Attacks
4. Email Content Interception
5. Email Header Manipulation
6. Denial of Service (DoS)
7. Man-in-the-Middle Attacks
8. Mailbombing
9. Unauthorized Access to Mailboxes

port 123 (NTP - Network Time Protocol):

1. NTP Amplification Attacks
2. Denial of Service (DoS)
3. Time Spoofing
4. Information Disclosure
5. Server Exploitation via Monlist Commands

port 143 (IMAP - Internet Message Access Protocol):

1. Email Account Compromise
2. Brute Force Attacks
3. Email Content Interception
4. Email Header Manipulation
5. Plain Text Authentication
6. Denial of Service (DoS)
7. Man-in-the-Middle Attacks
8. Unauthorized Access to Mailboxes

port 443 (HTTPS - Hypertext Transfer Protocol Secure):

1. SSL/TLS Vulnerabilities
2. Cross-Site Scripting (XSS)
3. SQL Injection
4. Cross-Site Request Forgery (CSRF)
5. Server Misconfigurations
6. Information Disclosure
7. Session Hijacking
8. Brute Force Attacks
9. Denial of Service (DoS)
10. Vulnerable Web Applications