Task 2 -

Port details

Port 20 - FTP DATA (process name) - TCP (Protocol used) - to send files between client and server (uses) - can be exploited with anonymous authentication , FTP login with anonymous(vulnerabilities)

Port 21 - FTP (process name) - TCP (Protocol used) - used for connection between 2 computers (uses) - can be exploited using brute force and anonymous authentication ,FTP login with anonymous (vulnerabilities)

Port 22 - SSH (process name) - TCP (Protocol used) - used for secure shell communication and allows remote administration access to the VM (uses) - can be exploited by tunneling random TCP traffic to other hosts on the network using Ruckus devices (vulnerabilities).

Port 23 - TELNET(process name)- TCP (Protocol used) - used by telnet protocol , commonly provides remote access to a variety of communications systems.(uses) - can be exploited using spoofing , credential sniffing and credential brute-forcing(vulnerabilities)

Port 25 - SMTP (process name)- TCP (Protocol used) - used for SMTP relaying ie, the transmission of email from email server to email server(uses) - vulnerable to mail spamming and spoofing (vulnerabilities)

Port 53 - DNS(process name)- TCP & UDP(Protocol used) - used for query and request information from DNS servers and server returns results to the client using same port (uses) - can be exploited by DDoS attacks (vulnerabilities)

Port 69 - TFTP(process name)- UDP (Protocol used) - used for booting UNIX or UNIX- like systems which do not have a local disk also known as netbooting. Also used for storing and retrieving files for devices such as Cisco routers and switches (uses)- can be exploited by remote attackers who can download server files without

authentication as it does not have encryption , access control or authentication (vulnerabilities)

Port 80 - HTTP(process name)- TCP & UDP(Protocol used) - used to send and receive unencrypted web pages (uses) - can be easily exploited because it’s not encrypted which makes it simple for cyber criminals to access , leak and tamper with sensitive data (vulnerabilities)

Port 110 - POP3(process name)- TCP (Protocol used) - used for unencrypted emails (uses) - can be easily exploited because it’s not encrypted (vulnerabilities)

Port 123 - NTP(process name)- TCP (Protocol used) - used for NTP communication , it provides time sync between computers (uses) - can be exploited using DoS because it relies on unauthenticated IPv4 time sources(vulnerabilities)

Port 143 - IMAP(process name)- TCP (Protocol used) - used to access email wherever you are from any device (uses) - can be exploited easily because it does not provide any default encryption (vulnerabilities)

Port 443 - HTTPS(process name)- TCP (Protocol used) - used for secure a communication channel between 2 devices (uses) - can be exploited by Man in the middle (MITM) attacks , malware infections where hackers can exploit and open ports to infect systems (vulnerabilities).