1. **Overall Vulnerability/Risk analysis 0.5p**

   Business risk (Executive summary)

   Leaked credentials pose a huge risk to the business. Sensitive information could be leaked and systems could be compromised. This could lead to legal issues and cause financial losses.

   Technical risk (Technical summary)

   Leaked credentials could give the attacker free reign on the company's systems. Sensitive information could be leaked and depending on the permission levels of the leaked user, the attacker could create a backdoor to allow them access even after the affected user's password is changed.

2. **Vulnerability impact review 0.5p**

   Risk likelihood

   Logging in with the leaked credentials is extremely easy. It is highly likely someone with little technical knowledge will try do it.

   Potential impact

   Impact of unauthorized access to the company's systems pose many risks. Sensitive data could be leaked, if the leaked credentials have root access to a system the whole network could be compromised. The business could face legal action for not storing their user credentials adequately.

3. **Remediation options 0.5p**
   Users should immediately change their passwords. Strict requirements for the passwords should be considered. The user credentials should be stored in an encrypted fashion instead of plaintext.

4. **Technical findings 2.5p**
   Running a nmap scan of the target IP reveals 6 open TCP ports. Most notably SSH server, http server, http proxy and an FTP server.

   The HTTP server is running on port 80. Telnet can be used to communicate with the server. Inputting “index.html HTTP/1.1” and “host: telnet” to the telnet console gives information about the running web server. A flag is found in the HTTP server header.

   The SSH server is running on port 22. Connecting to it with telnet shows the SSH server header. A flag is found there.

   An FTP server is running on port 10021. The server requires an username and a password. Seeing as two usernames have been leaked they can be used to try and gain access to the server. Running “hydra -l USERNAME -P rockyou.txt ftp://SERVER_IP:10021” will try to login to the ftp server using the given username and the passwords in the rockyou password list. Passwords are found for both of the usernames in the rockyou list. Logging in as “quinn” a file called “ftp_flag.txt” is found. The file contains the flag.

   Scanning the target server using nmap with the -sN option avoids detection by the IDS.

5. **Original cause 0.5p**
   There aren’t neccesarily any vulnerabilites detected expect for the leaked credentials. The IDS not detecting the Null Scan could be a problem if the desired function of the IDS is to prevent scanning completely.

6. **Conclusions 0.5p**

   Most likely compromise scenarios

   An attacket could easily scan the server with nmap and then connect to the FTP server with the leaked credentials. Most likely the attacker would be in search of any sensitive information.

Implications

The risk of leaked credentials is unauthorized access to the company's systems. The attacker can steal any data they want and could create a backdoor on the server to allow them access even after the affected users password is changed.

All user should change their password immediately following strict password requirements.

To combat credentials being leaked in the future, they should be stored in an encrypted fashion.