

# Trivial File Transfer Protocol (TFTP) Service

TFTP is a service that typically runs on UDP port 69. It is a file transfer service, but it does not allow listing of files



# Trivial File Transfer Protocol (TFTP) Service

So users who want to access files from a TFTP server must know the names of the files beforehand. From a security perspective, it's possible to bruteforce filenames on the server



# Trivial File Transfer Protocol (TFTP) Service

TFTP also allows file upload, so if files from the TFTP server are accessible via a web interface, the web app might be vulnerable to malicious file upload



# Privilege Escalation

## Sudo Html2text

html2text

 CI passing  codecov 97%

html2text is a Python script that converts a page of HTML into clean, easy-to-read plain ASCII text. Better yet, that ASCII also happens to be valid Markdown (a text-to-HTML format).

We have sudo access to the Html2text binary, which is a tool which converts HTML to ASCII text. This means we have privileged file read capability

# Privilege Escalation

## Sudo Html2text

html2text

 CI passing  codecov 97%

html2text is a Python script that converts a page of HTML into clean, easy-to-read plain ASCII text. Better yet, that ASCII also happens to be valid Markdown (a text-to-HTML format).

Which means we can read sensitive files such as `/etc/shadow` or root user SSH keys