TFTP Enumeration

Trivial File Transfer Protocol (TFTP) is a simple, connectionless file transfer protocol that is often used for booting diskless workstations, loading router configurations, and transferring files between systems. While TFTP can be a convenient way to transfer files, improper configuration can leave systems vulnerable to unauthorized access and exploitation.

TFTP Enumeration with Nmap

We will start off with nmap again to enumerate TFTP

```
nmap -Pn -sU -p69 -sV --script tftp-enum <IP>
```

Bad Luck, target is not running TFTP. Now, i tried to find a machine that has TFTP enable but i wasnt able to find any. But not issue with that, just keep the techniques in your notes and whenever you found this controversial port 69, just enumerate the hell out of it.

Checking if download/upload is possible using Metasploit

Moving on, Our good friend metasploit has a TFTP module named tftp_transfer_util that help us to check if download and upload is possible from the TFTP target server. Lets have a quick look on to it.

```
use auxiliary/admin/tftp/tftp_transfer_util
set RHOST <Target>
run
```
