NMAP

Script scans on 152.96.6.240 (step 7)

- anonymous FTP login allow: yes
- ftp version: vsFTPd 2.3.4
- OS: ubuntu804
- MYSQL is installed

Answers (step 8)

- Vulnerable hosts for EternalBlue: 152.96.6.249, 1522.96.6.251
- Full TCP scan: `nmap -sT ...` -> builds full TCP connection (and closes is, which is what distinguishes it from a half-open scan which leaves the TCP connection open)
- SYN scan: `nmap -sS ...` -> basically tries to establish TCP connection by sending a SYN flagged package and when we get an answer (ACK), the port is available
- half-open scan: `nmap -sS ...` -> sams as SYN Scan
- OS version: `nmap -O <target>` (`nmap -O -iL targets.txt`)
- Purpose of scripting: flexibility (e.g.: users can write their own script), specificaly target known vulnerabilities
- nmap scripts: `nmap --script-help "*"`
- access nmap stats during scan: