## 13-Hacking Web Servers

PLEASE use prebuilt labs

Victim Data: direct interaction Need 2-6 computers online that have the services running and vulnerable

**Advanced**: Build a data file / artifact that is actionable by the contract holder. There are no instructions for this task. You must figure everything out.
**Advanced:** capture encrypted packets, using decryption process from capture discussion

Attacker Data: Kali/ Parrot

Objective

Perform web server hacking:

- Footprint a web server using various information-gathering tools and inbuilt commands
- Enumerate web server information
- Crack remote passwords

Lab Tasks

Ethical hackers or pen testers use numerous tools and techniques to hack a target web server. Recommended labs that will assist you in learning various web server hacking techniques include:

1. Footprint the web server
    1.1. Information gathering using Ghost Eye
    1.2. Perform web server reconnaissance using Skipfish
    1.3. Footprint a web server using the httprecon Tool
    1.4. Footprint a web server using ID Serve
    1.5. Footprint a web server using Netcat and Telnet*
    1.6. Enumerate web server information using Nmap Scripting Engine (NSE)*
    1.7. Uniscan web server fingerprinting in Parrot Security
2. Perform a web server attack
    2.1. Crack FTP credentials using a Dictionary Attack*

*Indicates capture