# Ferramentas Week1 – Gh0styHunter

## Gobuster

- Função: Directory fuzzing / descoberta de páginas ocultas

- Comando básico usado:

gobuster -u http://fakebank.thm -w wordlists.txt dir

- Observações:

- Muito útil para reconhecimento inicial de Web Apps

- Salvar prints das execuções ajuda no portfólio

## Nmap

- Função: Reconhecimento de rede / descobrir portas e serviços

- Comandos básicos usados:

nmap -F <IP\_da\_VM>

nmap -p- <IP\_da\_VM>

nmap -sV -p22,80 <IP\_da\_VM>

- Observações:

- Essencial para mapear hosts antes de ataques

- Salvar prints das saídas ajuda no portfólio

## curl

- Função: Observar headers HTTP / respostas do servidor

- Comando básico usado:

curl -I http://<IP\_da\_VM>

- Observações:

- Permite analisar informações de segurança do servidor

- Importante para enumeração web inicial

## ffuf

- Função: Fuzzing de diretórios / descoberta de páginas ocultas

- Comando básico usado:

ffuf -u http://<IP\_da\_VM>/FUZZ -w /usr/share/wordlists/dirb/common.txt

- Observações:

- Mais rápido e flexível que Gobuster

- Permite filtrar status codes e salvar resultados

## burp suíte

- Burp Suite (Proxy, Repeater)

- Navegador (Chrome/Firefox)

- httpbin.org (teste seguro de requisições HTTP)

## Amass

- Código / Comando:

amass enum -d httpbin.org

- Função: enumeração de subdomínios ativos de um domínio (nenhum subdomínio encontrado)

##Ping

-Teste de conectividade (ICMP Echo Request/Reply).

##Telnet

-Conexão remota ao serviço exposto (porta 23/tcp).

##Shell Linux (bash)

-Interagir com o sistema e ler a flag (cat flag.txt).