Enumeração: Introdução

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Qual a importância?

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

+ Identificar detalhes do serviço em execução
+ Coletar mais informações do host
+ As informações complementares podem ajudar nas fases de exploração
+ A versão identificada pode ter uma vulnerabilidade conhecida (exploits públicos)
+ Alguns serviços podem ser vulneráveis a ataques de força bruta

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Qual o processo?

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

1. Identificar detalhes do serviço em execução
2. Estudar o serviço/protocolo para entender o funcionamento
3. Tentar interagir com o serviço/protocolo afim de obter mais informações do host
4. Identificar possíveis vulnerabilidades/ vetores de ataque

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

Exemplos

~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~

→ O serviço/protocolo quando mal configurado permite obter mais informações do host
→ O serviço/protocolo tem uma vulnerabilidade conhecida (pública)
→ O serviço/protocolo é vulnerável a um ataque de força bruta (tentativa e erro)
→ O serviço/protocolo tem uma vulnerabilidade desconhecida (0day)