

Metodologia Scanning

• ~~~~~

PROCESSO

~~~~~

- TCP HOST SCAN - Identificar todas as portas abertas (Protocolo TCP)
- UDP HOST SCAN - Identificar todas as portas abertas (Protocolo UDP)
- NETWORK SWEEPING - Identificar portas abertas na rede otimizando a busca
- Esse último é mais indicado quando estamos em uma rede com muitos computadores (tipo uns 5000). A análise de cada porta demoraria demais

~~~~~

DESAFIOS

~~~~~

- Tempo de scan e consumo do tráfego na rede
- Firewall Filtrando/ Rejeitando Pacotes
- Bloqueio de Portscan
- Sistemas de Detecção e Prevenção de Intrusos (IDS/IPS)