Professor
Edson Pedro FERLIN

Segurança da Informação

Pentest

Prof. Edson Pedro Ferlin

Professor
Edson Pedro FERLIN

Segurança da Informação

Pentest com nmap

Objetivo:
Mapear um host, identificar portas e serviços, e levantar possíveis vulnerabilidades.

Pré-requisito:
Fazer isso apenas em um IP que você **tem autorização para testar** (por exemplo, uma máquina virtual na sua rede).

Passo #1 - Descobrir hosts ativos na rede

nmap -sn 192.168.0.0/24

-sn → apenas ping scan (sem verificar portas)

Verifica quais IPs estão ativos na rede

Passo #2 - Varredura de portas padrão

nmap 192.168.0.105

Varre as 1000 portas mais comuns

Passo #3 - Varredura Completa de Portas

nmap -p- 192.168.0.105

-p- → varre todas as 65535 portas

Útil para achar serviços fora das portas padrão

Passo #4 - Identificar Serviços e Versões

nmap -sV 192.168.0.105

-sV → tenta identificar o software e a versão de cada serviço encontrado

Descobre software e versão de cada serviço

Passo #5 - Detecção de Sistema Operacional

nmap -O 192.168.0.105

-O → tenta identificar o sistema operacional

Tenta identificar o sistema operacional

Passo #6 - Scan com Scripts de Vulnerabilidade

nmap --script vuln 192.168.0.105

Busca vulnerabilidades conhecidas

Passo #7 - Scan Agressivo com Todas as Portas

nmap -A -p- 192.168.0.105

-A → ativa detecção de SO, versões, scripts e traceroute.
-p- → varre todas as portas

Combina várias detecções em um único comando

Passo #8 - Salvar Resultado em Arquivo

nmap -A -p- 192.168.0.105 -oN resultado.txt

Salva o resultado em um arquivo de texto

Relatório Final

O relatório deve conter:

- IP testado
- Portas abertas
- Serviços e versões
- Possíveis vulnerabilidades
- Recomendações

Contato

eferlin@live.com

(BLOG) professorferlin.blogspot.com

(SITE) professorferlin.com.br

(YOUTUBE) ProfEdsonPedroFerlin