ESCOLA ESTADUAL DE EDUCAÇÃO PROFISSIONAL DEPUTADO ROBERTO MESQUITA

Apresentação do trabalho de Segurança da Informação sobre: Nmap

Alunos: Glória Maria e Gustavo Almeida

O **Nmap** (Network Mapper) é uma ferramenta de código aberto amplamente utilizada para varredura de redes e auditoria de segurança. Ele foi projetado para ajudar administradores de sistemas e profissionais de segurança a identificar dispositivos e serviços em uma rede, além de analisar suas vulnerabilidades.

Principais Funções do Nmap

1. **Descoberta de Hosts**:
    - Permite identificar dispositivos ativos em uma rede.
    - Usa técnicas como ping e varreduras de portas para detectar a presença de hosts.
2. **Varredura de Portas**:
    - Identifica quais portas estão abertas em um dispositivo (e.g., portas 80 para HTTP, 443 para HTTPS).
    - Determina os serviços associados a essas portas.
3. **Identificação de Serviços e Versões**:
    - Descobre quais serviços estão sendo executados (e.g., Apache, MySQL).
    - Detecta as versões específicas dos serviços em execução.
4. **Sistema Operacional (OS) Detection**:
    - Analisa características da rede para estimar qual sistema operacional está sendo utilizado em um dispositivo.
5. **Scripts de Detecção de Vulnerabilidades (NSE - Nmap Scripting Engine)**:
    - Usa scripts personalizados para detectar vulnerabilidades conhecidas, realizar auditorias de segurança e automatizar testes.
6. **Mapeamento de Rede**:
    - Cria um diagrama lógico de uma rede com base nas informações coletadas, útil para análise e monitoramento.

Recursos e Características

- **Flexibilidade**: Suporta várias técnicas de varredura, como TCP SYN (rápida), TCP Connect, UDP, e muito mais.
- **Plataformas**: Funciona em Linux, Windows, macOS e outros sistemas operacionais.
- **Interface Gráfica**: Além da interface de linha de comando (CLI), há o **Zenmap**, uma interface gráfica para usuários que preferem uma experiência visual.
- **Personalização**: Com o NSE, usuários podem criar scripts para tarefas específicas, como identificar malware ou realizar verificações de conformidade.

Exemplos de Uso

Varredura Simples:
```
nmap 192.168.1.1
```

- Varredura básica de um host para descobrir portas abertas.

Varredura de Toda a Rede:
bash
Copiar código
```
nmap 192.168.1.0/24
```

- Identifica todos os dispositivos ativos em uma rede local.

Detecção de Sistema Operacional:
bash
Copiar código
```
nmap -O 192.168.1.1
```

- Tenta identificar o sistema operacional do host.

Varredura com NSE:
```
nmap --script vuln 192.168.1.1
```
Usa scripts NSE para identificar vulnerabilidades conhecidas.

Aplicações

- Testes de penetração e auditorias de segurança.
- Monitoramento de redes corporativas.
- Identificação de vulnerabilidades antes que sejam exploradas.
- Descoberta de dispositivos e inventário de ativos.

Embora seja uma ferramenta poderosa e versátil, o Nmap deve ser usado com responsabilidade, respeitando as permissões e políticas legais de uso.
