Manual de como usar a ferramenta Nikto

Autora: Deborah Bambil

Repositório oficial da ferramenta: https://www.cirt.net/Nikto2

Introdução

Nikto é uma ferramenta de scanner de vulnerabilidades para servidores web. Ela verifica um servidor em busca de vulnerabilidades conhecidas, configurações inadequadas e outros problemas de segurança.

Instalação

Em sistemas baseados em Debian/Ubuntu:

sudo apt update

sudo apt install nikto

Em sistemas baseados em Red Hat/CentOS:

sudo dnf install nikto

Via Git:

1. Clone o repositório oficial:

git clone https://github.com/sullo/nikto.git

2. Acesse a pasta clonada:

cd nikto/program

3. Torne o script executável:

chmod +x nikto.pl

Dependências:

Garanta que o Perl esteja instalado no sistema:

sudo apt install perl # Para sistemas Debian/Ubuntu

sudo dnf install perl # Para sistemas Red Hat/CentOS

Execução Básica

Para executar um escaneamento básico, use o comando:

nikto -h <URL ou IP>

Exemplo:

nikto -h https://exemplo.com

Comandos Principais

Especificar a porta:

nikto -h <IP ou URL> -p <PORTA>

Exemplo:

nikto -h https://exemplo.com -p 8080

Salvar os resultados:

nikto -h <URL ou IP> -output <arquivo>

Exemplo:

nikto -h https://exemplo.com -output resultado_nikto.txt

Utilizar proxy:

nikto -h <URL ou IP> -useproxy <endereço_proxy>

Exemplo:

nikto -h https://exemplo.com -useproxy http://127.0.0.1:8080

Desativar verificação SSL:

nikto -h <URL ou IP> -nossl

Exemplo:

nikto -h https://exemplo.com -nossl

Selecionar plugin:

nikto -h <URL ou IP> -Plugins <plugin>

Exemplo:

nikto -h https://exemplo.com -Plugins outdated

Especificar User-Agent:

nikto -h <URL ou IP> -useragent "<user_agent>"

Exemplo:

nikto -h https://exemplo.com -useragent "Mozilla/5.0"

Modo verbose:

nikto -h <URL ou IP> -Display V

Exemplo:

nikto -h https://exemplo.com -Display V

Testar apenas diretórios ou arquivos específicos:

nikto -h <URL ou IP> -Tuning <opções>

Exemplo (testar apenas diretórios):

nikto -h https://exemplo.com -Tuning 2

Exemplo de Comando Completo

Execução básica com saída para um arquivo:

nikto -h https://exemplo.com | tee resultado_nikto.txt

Dicas

- Sempre execute o Nikto em um ambiente autorizado.
- Use proxies e tune os parâmetros para otimizar a análise.
- Atualize o banco de dados do Nikto regularmente para garantir a detecção de novas vulnerabilidades.

perl nikto.pl -update
