Levantamento de vulnerabilidades com o Nikto;

localhost/

[[images/nikto.png]]

Introdução

O Nikto é uma ferramenta construida em Perl para avaliação de vulnerabilidades em servidores web, sua função é analisar e identificar falhas de segurança, principalmente aquelas que são baseadas em configuraçẽos default ou em mal uso de configurações e opções em uma plataforma.

Resumidamente as funções do Nikto são as seguintes:

- Análise de vulnerabilidades derivadas de falhas em configurações;
- Busca de arquivos de configuração default:
- Busca de arquivos considerados inseguros, devido a sua natureza, permissionamento etc;
- Busca por configurações e versões desatualizadas de softwares;

> *O nome "Nikto" veio do filme "O Dia em que a Terra Parou" versão original de 1951 e refilmagem em 2008, o nome em especifico é uma referência ao personagem "Klaatu barada nikto" interpretado originalmente por Michael Rennie e mais tarde na refilmagem por Keano Reeves;*

Executando o Nikto:

O Nikto é um recurso default no sistema operacional Kali, o qual será utilizado nestes testes, por ser uma ferramenta "command line" baseada em Perl pode ser executada a partir de qualquer plataforma que possua suporte a Linguagem, a ferramenta também possui suporte nativo a SSL e TLS além de opções para atuação via proxys e páginas autenticadas;

Caso precise você pode baixar o Nikto do Repositório do Projeto;

Para a sequencia de testes abaixo utilize como alvo o Metasploitable, substitua o endereço de destino para o endereço configurado em sua VM rodando o metasploitable;

Sintaxe Básica:

```
# nikto -H
```

A execução básica de um scan com o Nikto utiliza dois parâmetros: "-h" para host de destino e "-o" para geração de output que neste caso será no formato .html, outros formatos de sáida podem ser utilziados, são eles ".csv", ".txt" e ".xml".

```
# nikto -h 192.168.X.X -o result.html

...
- Nikto v2.1.6
```

```
---------------------------------------------------------------------------
+ Target IP:          192.168.X.X
+ Target Hostname:    192.168.X.X
+ Target Port:        80
+ Start Time:         2017-02-05 10:54:27 (GMT-2)
---------------------------------------------------------------------------
+ Server: Apache/2.2.8 (Ubuntu) DAV/2
+ Retrieved x-powered-by header: PHP/5.2.4-2ubuntu5.10
+ The anti-clickjacking X-Frame-Options header is not present.
+ The X-XSS-Protection header is not defined. This header can hint to the user
agent to protect against some forms of XSS
+ The X-Content-Type-Options header is not set. This could allow the user agent to
render the content of the site in a different fashion to the MIME type
+ Uncommon header 'tcn' found, with contents: list
+ Apache mod_negotiation is enabled with MultiViews, which allows attackers to
easily brute force file names. See
http://www.wisec.it/sectou.php?id=4698ebdc59d15. The following alternatives for
'index' were found: index.php
+ Apache/2.2.8 appears to be outdated (current is at least Apache/2.4.12). Apache
2.0.65 (final release) and 2.2.29 are also current.
+ Web Server returns a valid response with junk HTTP methods, this may cause false
positives.
+ OSVDB-877: HTTP TRACE method is active, suggesting the host is vulnerable to
XST
+ /phpinfo.php?VARIABLE=<script>alert('Vulnerable')</script>: Output from the
phpinfo() function was found.
+ OSVDB-3268: /doc/: Directory indexing found.
...
```

Escaneamento de portas diferentes e especificação de protocolo como SSL na porta 443:

```
# nikto -h 192.168.X.X -p 443  -ssl -o result.html
ou
# nikto -h https://192.168.X.X -ssl -o result.html
```

O Nikto também permite o uso de plugins específicos para escaneamento de vulnerabilidades especificas;

```
# nikto -list-plugins
```

Neste exemplo estou escaneando um avlo especificamente em busca de vulnerabilidades XSS:

```
# nikto -list-plugins | grep xss
# nikto -h 192.168.X.X -Plugins "apache_expect_xss(verbose,debug)" -o result.html
```

> *Por padrão o Nikto utilizará todos os plugins instalados, o uso de um plugin em especifico destina-se a restringir a busca quado teoricamente se tem uma noção mais exata do que se está procurando, no exemplo acima o plugin de XSS foi utilizado em modo debug gerando uma saída maior e mais especifica para este item em relação a saída padrão de um escaneamento geral, verifique a documentação oficial do nikto para um detalhamento melhor;*

Recursos úteis do Nikto:

Parâmetros:	Função:
-H:	Opções do Nikto, sintaxe básica;
-config :	Utilizar um arquivo base de configuração customizado no processo de scan;
-update:	Atualização de Plugins do Nikto;
-evasion:	Ṕermite a aplicação de configurações espcificas para "despistar" firewalls e soluções de IDS;
-Format: :	Formato de saída do relatório, este formato pode ser CSV, HTM, NBE (Nessus), SQL, TXT, ou XML;
-port :	Especificação do número da porta a ser utilizada no escaneamento;
-Plugins:	Definição do plugin de escaneamento a ser utilizado, por padrão o sistema utiliza o plugin default: ALL;
-list-plugins:	Lista de plugins disponíveis para uso;

> *A ideia de uma ferramenta que executa testes em vulnerabilidades conhecidas e brechas de configuração pode parecer simples, mas não é, é extremamente comum que se encontre configurações desatualizadas ou implementações simples sem qualquer nível de customização ou hardening;*

Material de Referência:

- Cirt.net Manuais de uso do Nikto

Free Software, Hell Yeah!