Fazendo varredura e levantando vulnerabilidades com Nikto

5 DE NOVEMBRO DE 2015

O Nikto é uma ferramenta em Perl desenvolvida por Chris Solo e David Lodge, a qual foi escrita para validação de vulnerabilidade suportando diversas plataformas, entre elas Windows, Linux e UNIX. Ao contrário de alguns scanners de segurança, o Nikto foi projetado para operar em um modo furtivo, mesmo assim ele causa um ruído como os demais scanners.

Ele é um scanner open source licenciado pela GPL, dentro de sua funções ele busca vulnerabilidades em seu alvo permitindo verificar nos servidores itens de configuração, como arquivos de índice, opções de servidor HTTP, identifica softwares instalados em servidores web e faz scan de itens e plugins que são frequentemente atualizados.

Algumas das características listada nela:

Suporte SSL (Unix com OpenSSL ou Windows com ActiveState's Perl/NetSSL).
Suporte a proxy HTTP completa.
Verifica a existência de componentes desatualizados do servidor.
Salvar os relatórios em texto simples, XML, HTML, CSV ou NBE.
Layout para personalização de relatórios.
Digitalizar várias portas em um servidor ou vários servidores via arquivo de entrada (incluindo saída do nmap).
Técnicas de codificação LibWhisker's IDS.
Update em linha de comando.
Identifica softwares instalados via cabeçalhos, ícones de favoritos e arquivos.
Autenticação da Host com Basic e NTLM.
Adivinhação de subdomínio.
Enumeração de usuários no Apache e cgiwrap.
Técnicas de "fish" para conteúdo em servidores web.
"Scan tuning" para incluir ou excluir entrada para checar classes vulneráveis.
Adivinha credenciais para autorização (incluindo muitos Id padrão e Pw combos).
Adivinha autorização lida em qualquer diretório, não apenas na raiz do diretório.
Redução de falsos positivos através de vários métodos: cabeçalhos, só conteúdo da página, e hashing do conteúdo.
Relatórios de cabeçalhos "incomuns".
Status interativo, pausa e alterações de configurações verbose.
Salvamento completo da requisição / resposta para os testes positivos.
Repetição salvada de solicitações positivas,
Tempo máximo de execução por alvo.

Pausa automática em um determinado momento.
Verifica a existência de sites em comuns em estado de “parking”.
Conexão com Metasploit.
Documentação completa.

Instalando o Nikto

Caso não tenha em sua distro, baixe a ferramenta feita pela nossa equipe: o Organon e instale-o. Caso queira instalar manualmente, siga os procedimentos abaixo.

Faça download do pacote:

```
# wget -cv http://www.cirt.net/nikto/nikto-2.1.5.tar.gz
```

O Nikto não precisa de compilação, descompacte ele e entre na pasta.

```
# tar -xvzf nikto-2.1.5.tar.gz
```

```
# cd nikto-2.1.5/
```

Dê permissão para executar o arquivo.

```
# chmod 777 nikto.pl
```

Atualize a ferramenta para a versão mais recente caso tenha disponível.

```
# ./nikto.pl -update
```

Realizando teste com Nikto

Antes de iniciar o *scanning* com a ferramenta, precisamos conhecer as informações de configurações que tem disponível na ferramenta para auxiliar melhor o entendimento dela. Para ver as suas opções digite o comando de ajuda, listado logo abaixo.

```
# ./nikto -h
```

Iremos fazer algumas demonstrações específicas para realizar scans num determinado alvo:

```
# ./nikto.pl -host http://testphp.vulnweb.com/ -p 80,443 -o relatorio.txt
```

Onde:

-host: endereço da vítima (IP ou DNS), nesse caso pegaremos um site próprio para teste.
-p: porta para efetuar o scan, de preferência faça scan antes para ver as portas que estão rodando serviços web.
-o: saída do arquivo (log do scan).

Podemos fazer uma análise mais profunda no site.

```
# ./nikto.pl -C all -host http://testphp.vulnweb.com/ -p 80,443 -mutate 1,2,3,4 -evasion 1,2 -o relatorio.txt
```

Onde:

-mutate 1,2,3,4: busca por diretório através de tentativas exaustivas (causa bastante ruído).
-evasion 1,2: faz scan fica mais furtivo, burlando alguns tipos firewall e IPS.
-C all: força a checagem de todos os diretórios em busca de CGI.

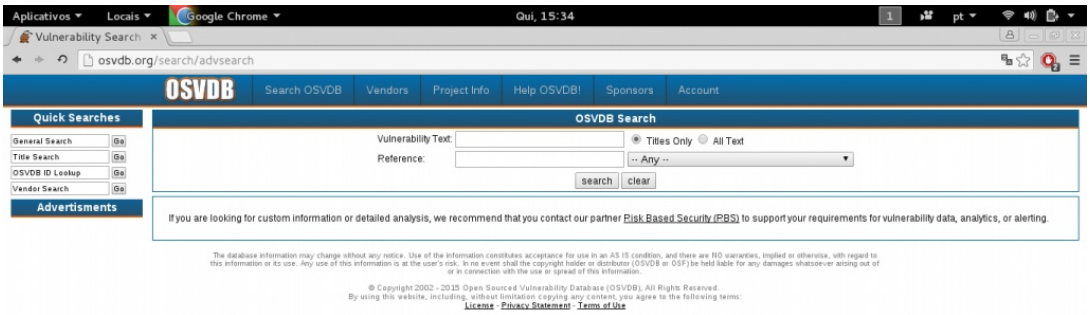
```
- Nikto v2.1.6
---------------------------------------------------------------------------
+ Target IP:          176.28.50.165
+ Target Hostname:    testphp.vulnweb.com
+ Target Port:        80
+ Start Time:         2015-11-05 14:53:46 (GMT-2)
---------------------------------------------------------------------------
+ Server: nginx/1.4.1
+ Retrieved x-powered-by header: PHP/5.3.10-1~lucid+2uwsgi2
+ 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 t
ype
+ Server leaks inodes via ETags, header found with file /clientaccesspolicy.xml, fields: 0x5049b03d 0x133
+ /clientaccesspolicy.xml contains a full wildcard entry. See http://msdn.microsoft.com/en-us/library/cc197955(v=vs.95).aspx
+ lines
+ /crossdomain.xml contains a full wildcard entry. See http://jeremiahgrossman.blogspot.com/2008/05/crossdomainxml-invites-cross-site.html
+ /CVS/Entries: CVS Entries file may contain directory listing information.
+ OSVDB-3268: /admin/: Directory indexing found.
+ OSVDB-12184: /?=PHPB8B5F2A0-3C92-11d3-A3A9-4C7B08C10000: PHP reveals potentially sensitive information via certain HTTP requests that contain specif
ic QUERY strings.
+ OSVDB-12184: /?=PHPE9568F36-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specif
ic QUERY strings.
+ OSVDB-12184: /?=PHPE9568F34-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specif
ic QUERY strings.
+ OSVDB-12184: /?=PHPE9568F35-D428-11d2-A769-00AA001ACF42: PHP reveals potentially sensitive information via certain HTTP requests that contain specif
ic QUERY strings.
+ OSVDB-3092: /admin/: This might be interesting...
+ OSVDB-3268: /images/: Directory indexing found.
+ OSVDB-3268: /images/?pattern=/etc/*&sort=name: Directory indexing found.
```

Como sempre, se recomenda a utilização de proxy para fazer scan, para caso ele bloqueie você não fique impossibilitado de continuar fazendo no seu IP outros tipos de varredura. A opção **-useproxy** permite você adicionar um, como exemplo o privoxy ou TOR.

```
# ./nikto.pl -C all -host http://testphp.vulnweb.com/ -p 80,443 -mutate 1,2,3,4 -evasion 1,2 -o relatorio.txt -useproxy 127.0.0.1
```

Fomos incrementando aos poucos os comandos para que você entenda como refinar o scan, lembrando que é de extrema importância que você leia a documentação dele para aprender como usar outras configurações de scan.

As vulnerabilidades e avisos listados no arquivo que é gerado pelo scan (log) são catalogadas de acordo com o banco de dados OSVDB, que pode ser acessado aqui e poderá encontrar sobre os detalhes de cada vulnerabilidade citada pelo Nikto, e explorá-las.



Basta colocar o número da falha nomeada no OSVDB que trará as informações correspondente na pesquisa.

Conclusão

O Nikto é muito utilizado como scanner atualmente, tendo a principal característica suas técnicas de furtividades durante seu scan, burlando alguns tipos de IPS e firewalls. Não possui uma interface gráfica tão explicativa como entre outros scanner como Nessus ou Acunetix, por isso é necessário visitar o catalogo da OSVDB para ver todas as informações da falha. Lembrando que como qualquer outro scanner ele gera ruido, mas tem a opção de amenizar devido a suas configurações de evasão como já dito.

Indicação de leitura complementar

https://www.viazap.com.br/?p=1297

Green Hat, Pentest, Scanners

INSTALANDO NIKTO NIKTO NIKTO SCANNER VARREDURA COM NIKTO