

Индивидуальный проект. Этап 4

Использование nikto

Дарья Эдуардовна Ибатулина

Содержание

1	Цель работы	5
2	Задание	6
3	Теоретическое введение	7
4	Выполнение лабораторной работы	9
5	Выводы	13
	Список литературы	14

Список иллюстраций

4.1	Справка по <code>nikto</code>	9
4.2	Сканирование сайта мэра Москвы	10
4.3	Сканирование сайта <i>pbs.org</i> с SSL	10
4.4	Сканирование IP-адреса с помощью <code>ifconfig</code>	11
4.5	Использование <code>IpCalc</code> для IP-адреса	12

Список таблиц

1 Цель работы

Целью работы являются: получение знаний о том, для чего используется nikto, сканирование веб-сайта, поиск уязвимостей в нем.

2 Задание

1. Вызвать справку по nikto;
2. Просканировать любой сайт;
3. Просканировать любой сайт с ssl4
4. Выяснить свой IP-адрес.

3 Теоретическое введение

Перед тем как атаковать любой сайт, хакер или пентестер сначала составляет список целей. После того, как он проведет хорошую разведку и найдет слабые места для «наведения прицела», ему понадобится инструмент сканирования веб-сервера, такой как Nikto, который поможет найти уязвимости – потенциальные вектора атаки.

Nikto – это простой открытый сканер веб-серверов, который проверяет веб-сайт и сообщает о найденных уязвимостях, которые могут быть использованы для эксплойта или взлома. Кроме того, это один из наиболее широко используемых инструментов сканирования веб-сайтов на уязвимости во всей отрасли, а во многих кругах он считается отраслевым стандартом.

Несмотря на то, что этот инструмент чрезвычайно эффективен, он не действует скрытно. Любой сайт с системой обнаружения вторжений или иными мерами безопасности поймет, что его сканируют. Nikto был разработан для тестирования безопасности и о скрытности его работы никто не задумывался.

Как правильно использовать Nikto

Если вы просто запустите Nikto на целевом веб-сайте, вы, возможно, не поймете, что делать с информацией, полученной после сканирования. Nikto на самом деле больше похож на лазерную указку, которая влечет за собой выстрел, и через некоторое время вы увидите, как это работает.

Для начала давайте поговорим о целях (target). Целью может оказаться почти любое место, куда может нанести свой удар хакер, например, сетевые принтеры или веб-сервер. Когда мы чуть позже перейдем к использованию Nikto, нам

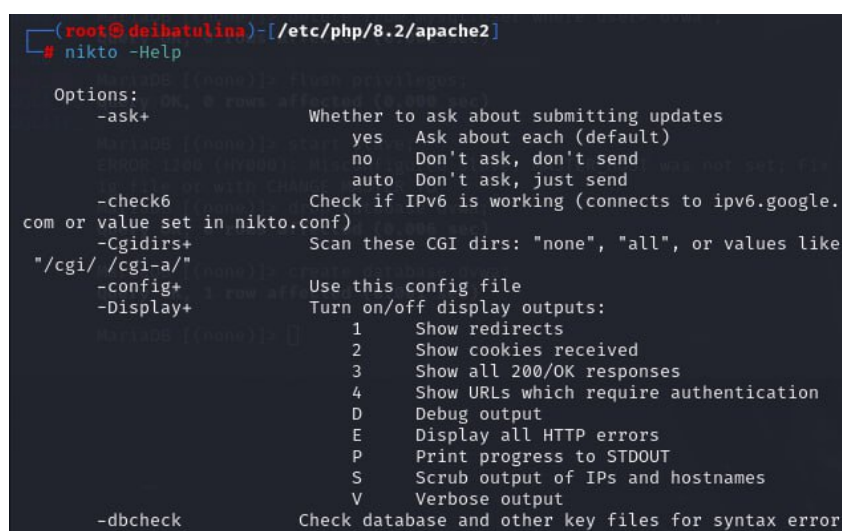
нужно будет предоставить ему один из трех видов информации: IP-адрес для локальной службы, веб-домен для атаки или веб-сайт SSL/HTTPS.

Прежде чем начинать сканирование с помощью Nikto, лучше предварительно провести разведку с помощью такого открытого инструмента как Maltego. Такие инструменты могут оказаться полезными при создании профиля и формировании более конкретного списка целей, на которых стоит сосредоточиться. Как только вы это сделаете, можно будет воспользоваться Nikto для поиска потенциальных уязвимостей в целях из вашего списка.

Если повезет, уязвимость с известным эксплойтом будет найдена, а значит, что уже существует инструмент, который поможет воспользоваться этим слабым местом. С помощью соответствующего инструмента, который автоматически эксплуатирует уязвимость, хакер может получить доступ к цели для выполнения любого количества скрытых атак, таких как, например, добавление вредоносного кода [1].

4 Выполнение лабораторной работы

1. Для начала следует установить nikto. Однако, я использую дистрибутив Kali Linux, а в нем nikto уже предустановлен. Чтобы в этом убедиться, вызову справку командой `nikto -Help` (рис. [4.1]).



```
(root@deibatulina)-[/etc/php/8.2/apache2]
# nikto -Help

Options:
-ask+          Whether to ask about submitting updates
                yes   Ask about each (default)
                no    Don't ask, don't send
                auto   Don't ask, just send
-check6        Check if IPv6 is working (connects to ipv6.google.
com or value set in nikto.conf)
-Cgidirs+      Scan these CGI dirs: "none", "all", or values like
"/cgi/" /cgi-a/"
-config+       Use this config file
-Display+      Turn on/off display outputs:
                1     Show redirects
                2     Show cookies received
                3     Show all 200/OK responses
                4     Show URLs which require authentication
                D     Debug output
                E     Display all HTTP errors
                P     Print progress to STDOUT
                S     Scrub output of IPs and hostnames
                V     Verbose output
-dbcheck       Check database and other key files for syntax error
```

Рис. 4.1: Справка по nikto

2. Затем для классического сканирования сайта буду использовать базовый синтаксис `nikto -h <IP или hostname>` с фактическим IP-адресом или именем хоста без угловых скобок. Просканирую таким образом сайт мэра Москвы (рис. [4.2]).

```
deibatulina@deibatulina: ~  
File Actions Edit View Help  
$ nikto -h mos.ru  
- Nikto v2.5.0  
  
+ Target IP: 94.79.51.169  
+ Target Hostname: mos.ru  
+ Target Port: 80  
+ Start Time: 2024-04-27 19:20:54 (GMT3)  
  
+ Server: nginx  
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options  
+ /: 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. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/  
+ Root page / redirects to: https://mos.ru/  
+ [[B^[[B^[[B+ No CGI Directories found (use '-C all' to force check all possible dirs)  
+ ERROR: Error limit (20) reached for host, giving up. Last error: error reading HTTP response  
+ Scan terminated: 19 error(s) and 2 item(s) reported on remote host  
+ End Time: 2024-04-27 19:23:55 (GMT3) (181 seconds)  
  
+ 1 host(s) tested  
  
(deibatulina@deibatulina)-[~]  
$
```

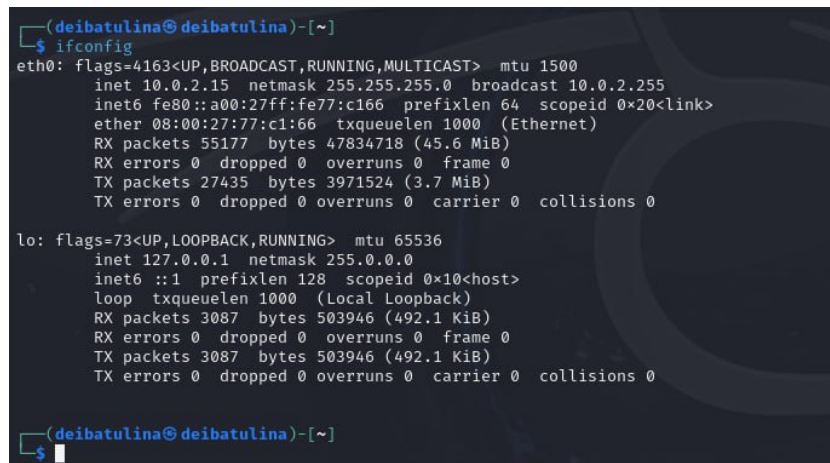
Рис. 4.2: Сканирование сайта мэра Москвы

3. Далее, сканирую сайт *pbs.org* с SSL `nikto -h pbs.org -ssl` (рис. [4.3]).

```
(deibatulina@deibatulina)-[~]  
$ nikto -h pbs.org -ssl  
- Nikto v2.5.0  
  
+ Multiple IPs found: 54.225.206.152, 54.225.198.196  
+ Target IP: 54.225.206.152  
+ Target Hostname: pbs.org  
+ Target Port: 443  
  
+ SSL Info: Subject: /CN=www.pbs.org  
Ciphers: ECDHE-ECDSA-AES128-GCM-SHA256  
Issuer: /C=US/O=Let's Encrypt/CN=R3  
+ Start Time: 2024-04-27 19:26:20 (GMT3)  
  
+ Server: openresty  
+ /: The anti-clickjacking X-Frame-Options header is not present. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/X-Frame-Options  
+ /: Uncommon header 'x-pbs-fwsrvname' found, with contents: ip-10-193-148-58.ec2.internal.  
+ /: The site uses TLS and the Strict-Transport-Security HTTP header is not defined. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Strict-Transport-Security  
+ /: 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. See: https://www.netsparker.com/web-vulnerability-scanner/vulnerabilities/missing-content-type-header/  
+ Root page / redirects to: https://www.pbs.org/  
+ No CGI Directories found (use '-C all' to force check all possible dirs)  
+ /: Uncommon header 'x-cache-fs-status' found, with contents: EXPIRED.  
+ Hostname 'pbs.org' does not match certificate's names: www.pbs.org. See: https://cwe.mitre.org/data/definitions/297.html
```

Рис. 4.3: Сканирование сайта *pbs.org* с SSL

4. Теперь, когда я провела быстрое сканирование веб-сайта, можно попробовать использовать Nikto в локальной сети, чтобы найти embedded-сервера, такие как страница логина роутера или HTTP-сервис на другой машине, который представляет из себя просто сервер без веб-сайта. Чтобы узнать IP-адрес, я буду использовать ifconfig: ifconfig (рис. [4.4]).



```
(deibatulina@deibatulina)-[~]
$ ifconfig
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
    inet 10.0.2.15 netmask 255.255.255.0 broadcast 10.0.2.255
    inet6 fe80::a00:27ff:fe77:c166 prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:77:c1:66 txqueuelen 1000 (Ethernet)
    RX packets 55177 bytes 47834718 (45.6 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 27435 bytes 3971524 (3.7 MiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

lo: flags=73<UP,LOOPBACK,RUNNING> mtu 65536
    inet 127.0.0.1 netmask 255.0.0.0
    inet6 ::1 prefixlen 128 scopeid 0x10<host>
    loop txqueuelen 1000 (Local Loopback)
    RX packets 3087 bytes 503946 (492.1 KiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 3087 bytes 503946 (492.1 KiB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

(deibatulina@deibatulina)-[~]
$
```

Рис. 4.4: Сканирование IP-адреса с помощью ifconfig

5. IP-адрес, который мне нужен, относится к «inet». На нем можно использовать ipcalc для того, чтобы получить сетевой диапазон. Если у ipcalc не установлен, необходимо установить его с помощью команды apt install ipcalc, а затем повторить попытку. Диапазон будет стоять после «Network», в моем случае это 10.0.2.15 (рис. [4.5]).

```
(deibatulina@deibatulina)-[~]
$ ipcalc 10.0.2.15
Command 'ipcalc' not found, but can be installed with:
sudo apt install ipcalc
Do you want to install it? (N/y)y
sudo apt install ipcalc
[sudo] password for deibatulina:
Sorry, try again.
[sudo] password for deibatulina:
Reading package lists... Done
Building dependency tree... Done
Reading state information... Done
The following NEW packages will be installed:
  ipcalc
0 upgraded, 1 newly installed, 0 to remove and 267 not upgraded.
Need to get 26.3 kB of archives.
After this operation, 74.8 kB of additional disk space will be used.
Get:1 http://kali.download/kali kali-rolling/main amd64 ipcalc all 0.51-1 [26.3 kB]
Fetched 26.3 kB in 0s (53.3 kB/s)
Selecting previously unselected package ipcalc.
(Reading database ... 403891 files and directories currently installed.)
Preparing to unpack .../archives/ipcalc_0.51-1_all.deb ...
Unpacking ipcalc (0.51-1) ...
Setting up ipcalc (0.51-1) ...
Processing triggers for man-db (2.12.0-3) ...
Processing triggers for kali-menu (2023.4.7) ...

(deibatulina@deibatulina)-[~]
$
```

Рис. 4.5: Использование IpCalc для IP-адреса

5 Выводы

В результате выполнения лабораторной работы я получила практические навыки работы с nikto, а также узнала, для чего он используется.

Список литературы

[1] Статья: Проверяем на уязвимости любой сайт с помощью Nikto. URL: <https://habr.com/ru/companies/otus/articles/492546/> [Дата обращения 27.04.2024]