

Индивидуальный проект этап 5

Использование Burp Suite

Неустроева Ирина Николаевна

Содержание

1	Теоретическое введение	5
2	Цель работы	7
3	Задание	8
4	Выполнение	9
5	Выводы	12

Список иллюстраций

4.1	Знакомство с Nikto	9
4.2	Базовое сканирование сайта	10
4.3	Сканирование сайта pbc.org	10
4.4	Сканирование IP-адреса с помощью ifconfig	11
4.5	Использование IpCalc для IP-адреса	11

Список таблиц

1 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.

2 Цель работы

Приобретение практических навыков по использованию инструмента Nikto для сканирования веб-сайтов и поиска уязвимости в нем

3 Задание

1. Вызвать справку по nikto
2. Просканировать сайт
3. Просканировать сайт с ssl
4. Выяснить свой ip-адрес

4 Выполнение

1. Перед сканированием веб-серверов использовали параметр -Help, чтобы увидеть, что можно делать с этим инструментом

```
(inneustroeva@inneustroeva)-[~]
$ 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
s
  -evasion+       Encoding technique:
                   1     Random URI encoding (non-UTF8)
```

Рис. 4.1: Знакомство с Nikto

2. Затем используем базовый синтаксис `nikto -h` для классического сканирования сайта. Таким образом мы просканировали сайт `rudn.ru`

```

~$ nikto -h rudn.ru
- Nikto v2.5.0

+ Target IP:      185.178.208.57
+ Target Hostname: rudn.ru
+ Target Port:    80
+ Start Time:     2025-05-01 14:08:26 (GMT3)

+ Server: ddos-guard
+ /: 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/
+ /: Cookie __ddg8_ created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: Cookie __ddg10_ created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: Cookie __ddg9_ created without the httponly flag. See: https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies
+ /: IP address found in the '__ddg9_' cookie. The IP is "46.147.148.170".
+ Root page / redirects to: https://rudn.ru/
+ /cvIjV3kF.TXT: Uncommon header 'ddg-cache-status' found, with contents: MIS S.
+ No CGI Directories found (use '-C all' to force check all possible dirs)
+ : Server banner changed from 'ddos-guard' to 'ngjit'.

```

Рис. 4.2: Базовое сканирование сайта

3. Далее сканирую сайт pbs.org с SSL “nikto -h -ssl”

```

~$ 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=E6
+ Start Time:    2025-05-01 14:12:44 (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-kids-map' found, with contents: nousername.
+ /: Uncommon header 'x-pbs-fwsrvname' found, with contents: ip-10-193-194-159.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/

```

Рис. 4.3: Сканирование сайта pbs.org

4. Теперь, когда мы провели 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 сервис без веб-сайта,
Чтобы узнать IP-адрес, я буду использовать ifconfig

```
(inneustroeva@inneustroeva)-[~]
$ 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:fea0:befb prefixlen 64 scopeid 0x20<link>
    ether 08:00:27:a0:be:fb txqueuelen 1000 (Ethernet)
    RX packets 11014 bytes 5898691 (5.6 MiB)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 8158 bytes 1212261 (1.1 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 8 bytes 480 (480.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 8 bytes 480 (480.0 B)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

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

Рис. 4.4: Сканирование IP-адреса с помощью ifconfig

5. IP-адрес, который нам нужен относится к inet. На нем мы можем использовать ipcalc Диапазон будет стоять после Network, в нашем случае это 10.0.2.255

Использование IpCalc для IP-адреса

Рис. 4.5: Использование IpCalc для IP-адреса

5 Выводы

В ходе нашей работы, приобрела практические навыки по использованию инструмента Nikto для сканирования веб-сайтов и поиска уязвимости в нем.