

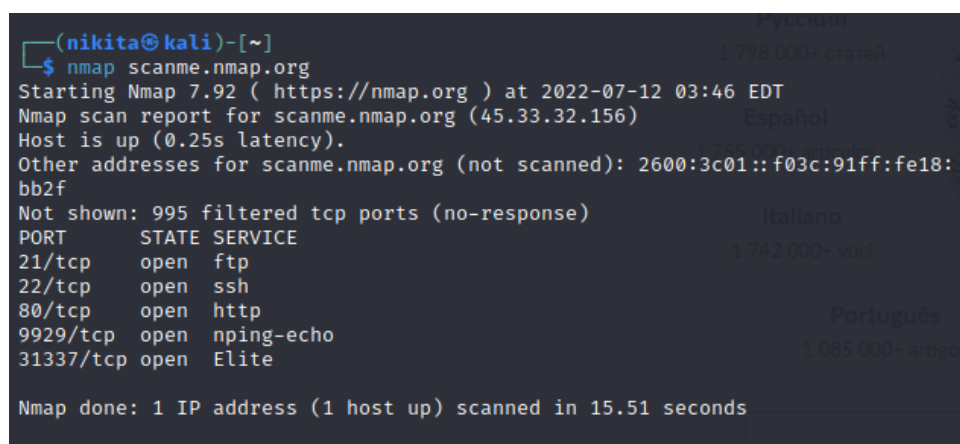
Практические навыки работы с Kali Linux

На основе операционной системы Kali Linux были разобраны основные инструменты для проведения тестирований на проникновение. Попробуем найти какие-либо данные с помощью его инструментов. Kali имеет широкий спектр программ для сканирования хостов на наличие открытых портов и анализ уязвимостей веб-серверов.

Nmap

Nmap— утилита, предназначенная для сканирования IP-сетей, определения состояния объектов сканируемой сети (портов и соответствующих им служб).

Первым делом просканируем специальный хост на наличие открытых портов (см. рисунки 1).



```
(nikita@kali)~$ nmap scanme.nmap.org
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-12 03:46 EDT
Nmap scan report for scanme.nmap.org (45.33.32.156)
Host is up (0.25s latency).
Other addresses for scanme.nmap.org (not scanned): 2600:3c01::f03c:91ff:fe18:bb2f
Not shown: 995 filtered tcp ports (no-response)
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http
9929/tcp  open  nping-echo
31337/tcp open  Elite

Nmap done: 1 IP address (1 host up) scanned in 15.51 seconds
```

Рисунок 1 – Сканирование хоста scanme.nmap.org

Анализируем полученные данные:

1. Разберемся с состояниями (STATE)

Nmap распознаёт следующие состояния портов: open, filtered, closed, или unfiltered. Open - готово для принятия пакетов на этот порт. Filtered -брандмауэр, фильтр, или что-то другое в сети блокирует порт, так что Nmap не может определить, является ли порт открытым или закрытым. Closed — не связаны в данный момент ни с каким приложением, но могут быть открыты в любой момент. Unfiltered порты отвечают на запросы Nmap, но нельзя определить, являются ли они открытыми или закрытыми.

2. Service и port

Стандартные сервисы находятся на своих стандартных портах:

FTP — протокол передачи файлов по сети.

SSH — сетевой протокол прикладного уровня, позволяющий производить удалённое управление операционной системой и туннелирование TCP-соединений.

HTTP - протокол прикладного уровня передачи данных.

И пару нестандартных соединений:

Nping — это инструмент с открытым исходным кодом для генерации сетевых пакетов, анализа ответов и измерения времени отклика.

31337 - Этот номер порта означает «элитный» в написании взломщика (3=E, 1=L, 7=T) и из-за особого значения часто используется для целей злоумышленников. На этом порту работает много бэкдоров/троянов, вот некоторые другие, которые работают на том же порту: Back Orifice, Elite.

Таким образом, мы нашли бэкдор¹.

Nikto

Nikto – это инструмент оценки веб-серверов. Он предназначен для поиска различных небезопасных файлов, конфигураций и программ на веб-серверах любого типа. Результат работы сканера показан на рисунке 2.

¹ **Backdoor** — вредоносная программа, которая предоставляет доступ к устройству для несанкционированных действий. Бэкдор в точности соответствует своему названию (от англ. back door — «черный ход»): скрытно впускает злоумышленника в систему.

```
(root@kali)-[~]
# nikto -h pbs.org -ssl
- Nikto v2.1.6

+ Target IP: 54.225.206.152
+ Target Hostname: pbs.org
+ Target Port: 443

+ SSL Info: Subject: /CN=www.pbs.org
            Ciphers: ECDHE-RSA-AES128-GCM-SHA256
            Issuer: /C=US/O=Let's Encrypt/CN=R3
+ Message: Multiple IP addresses found: 54.225.206.152, 54.225.198.196
+ Start Time: 2022-07-12 04:27:50 (GMT-4)

+ Server: openresty
+ 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
+ Uncommon header 'x-pbs-fwsrvname' found, with contents: ip-10-193-16-94.ec2.internal
+ The site uses SSL and the Strict-Transport-Security HTTP header is not defined.
+ The site uses SSL and Expect-CT header is not present.
+ 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
+ Root page / redirects to: https://www.pbs.org/
```

Рисунок 2 – Вывод команды от сканера Nikto.

Этой командой мы сразу получаем особенности структуры сайта, благодаря информации о заголовках и сервере. Стоит отметить, что Nikto имеет широкий функционал и способен частично или полностью заменять другие инструменты. Так, например, он также выдает информацию о протоколах шифрования SSL, таким образом мы можем не прибегать без необходимости к Wireshark²-у.

Sublister

Sublister — это инструмент, разработанный на Python для поиска поддоменов веб-сайта с использованием OSINT³.

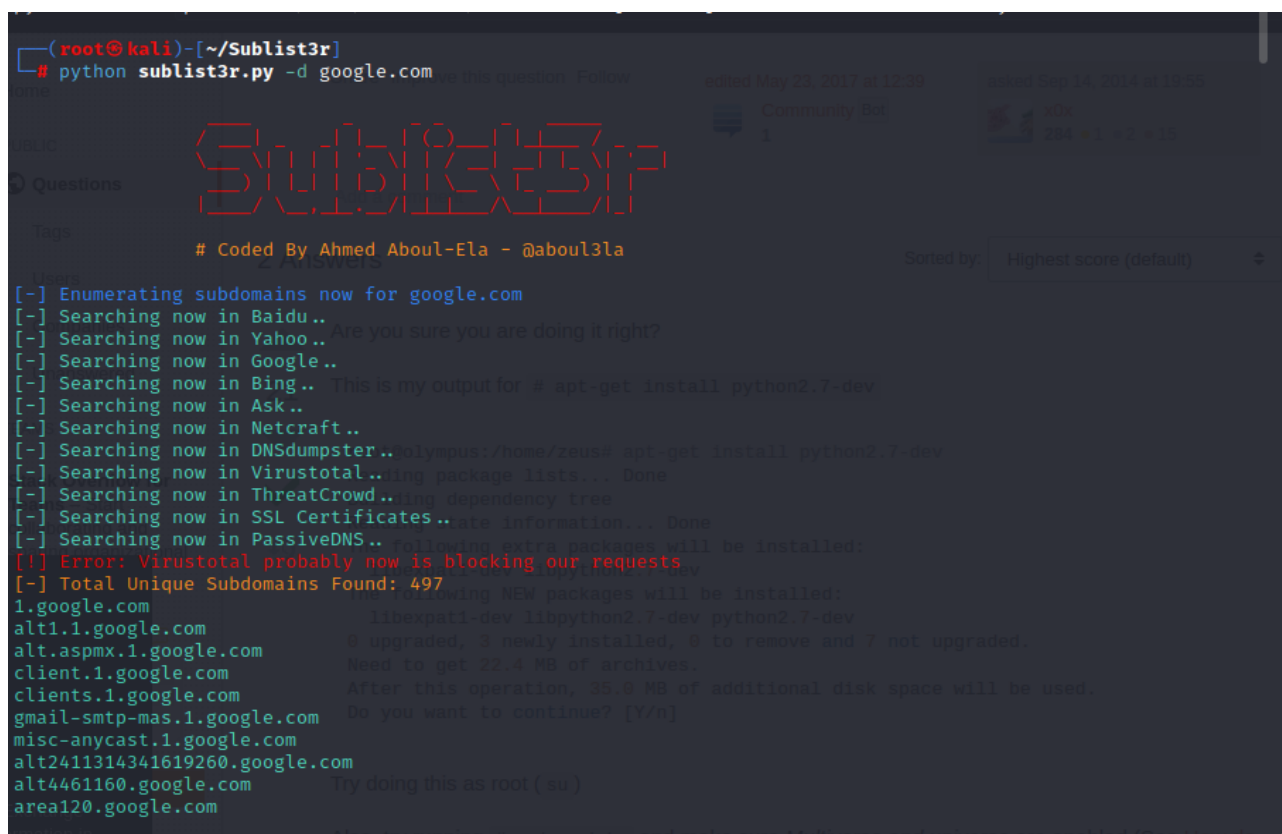
Для начала разберемся с основными понятиями. Название сайта

² Wireshark — программа-анализатор трафика для компьютерных сетей Ethernet и некоторых других.

³ OSINT-разведывательная дисциплина, включающая в себя поиск, выбор и сбор разведывательной информации из общедоступных источников, а также её анализ

соотнесенное по DNS с IP-адресом называется доменом. Поддомен же нужен для продвижения сайтов и разветвления тяжелой структуры сайта. В пентесте необходим поиск поддоменов для тестирования на безопасность, ведь поддомен может оказаться слабо защищенным.

Попробуем найти поддомены google.com. Для этого воспользуемся программой для поисков поддоменов Sublist3r (см. рисунки 3).



```
(root@kali)-[~/Sublist3r]
# python sublist3r.py -d google.com

Sublist3r
# Coded By Ahmed Aboul-Ela - @aboul3la

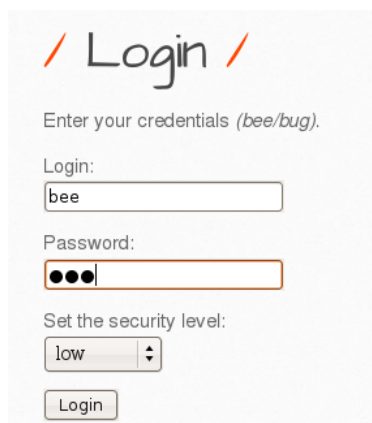
[-] Enumerating subdomains now for google.com
[-] Searching now in Baidu..
[-] Searching now in Yahoo.. Are you sure you are doing it right?
[-] Searching now in Google..
[-] Searching now in Bing.. This is my output for # apt-get install python2.7-dev
[-] Searching now in Ask..
[-] Searching now in Netcraft..
[-] Searching now in DNSdumpster..
[-] Searching now in Virustotal..
[-] Searching now in ThreatCrowd..
[-] Searching now in SSL Certificates..
[-] Searching now in PassiveDNS..
[!] Error: Virustotal probably now is blocking our requests
[-] Total Unique Subdomains Found: 497
1.google.com
alt1.1.google.com
alt.aspmx.1.google.com
client.1.google.com
clients.1.google.com
gmail-smtp-mas.1.google.com
misc-anycast.1.google.com
alt2411314341619260.google.com
alt4461160.google.com
area120.google.com
```

Рисунок 3 –Найденные поддомены сайта google.com.

Фреймворк Metasploit

Metasploit - Фреймворк для тестирования на проникновение [6]. Для тестирования фреймворка установим bee-box (виртуальная машина с предустановленным bWAPP-ом⁴). На рисунке 4 видно поле настроек bWAPP.

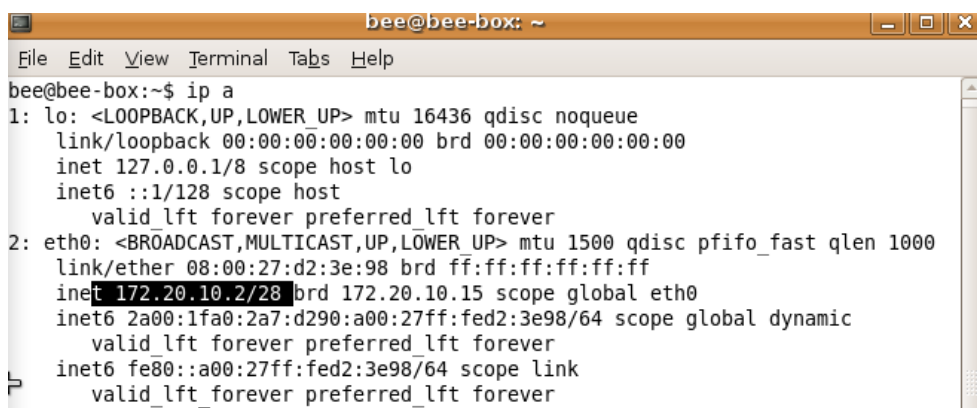
⁴ bWAPP- намеренно небезопасное веб-приложение с открытым исходным кодом. Содержит около ста уязвимостей по топ-10 от OWASP, упоминаемый ранее в этапе 3.



A login form titled "Login" with a stylized orange slash on either side. Below the title, it says "Enter your credentials (bee/bug)". There are two input fields: "Login:" with the text "bee" entered, and "Password:" with four black dots. Below these is a "Set the security level:" section with a dropdown menu showing "low". At the bottom is a "Login" button.

Рисунок 4 –Настройки bWAPP

Далее определим IP нашей машины и зайдём на него. Мы достигли этого благодаря типу подключения – сетевой мост. IP машины и процесс подключения к ней можно увидеть на рисунках 5 и 6.



```
bee@bee-box: ~  
File Edit View Terminal Tabs Help  
bee@bee-box:~$ ip a  
1: lo: <LOOPBACK,UP,LOWER UP> mtu 16436 qdisc noqueue  
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00  
    inet 127.0.0.1/8 scope host lo  
    inet6 ::1/128 scope host  
        valid_lft forever preferred_lft forever  
2: eth0: <BROADCAST,MULTICAST,UP,LOWER UP> mtu 1500 qdisc pfifo_fast qlen 1000  
    link/ether 08:00:27:d2:3e:98 brd ff:ff:ff:ff:ff:ff  
    inet 172.20.10.2/28 brd 172.20.10.15 scope global eth0  
    inet6 2a00:1fa0:2a7:d290:a00:27ff:fed2:3e98/64 scope global dynamic  
        valid_lft forever preferred_lft forever  
    inet6 fe80::a00:27ff:fed2:3e98/64 scope link  
        valid_lft forever preferred_lft forever
```

Рисунок 5–IP машины

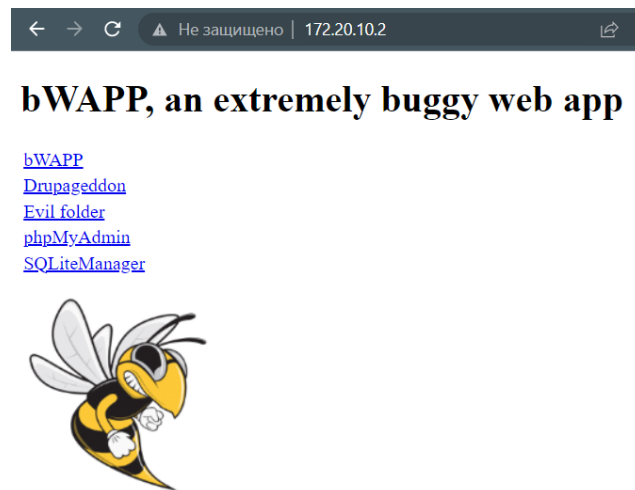


Рисунок 6- Подключение к bee-box по IP
Настройки виртуальной машины приведены на рисунке 7.

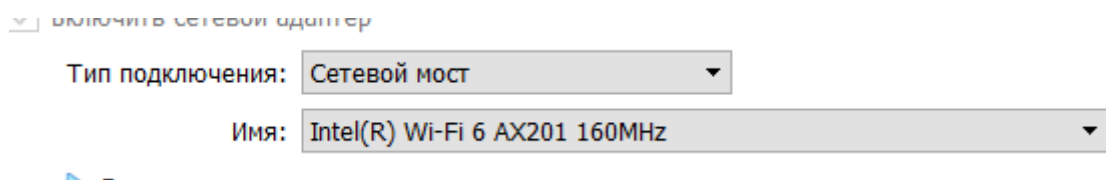


Рисунок 7–Настройки VirtualBox для машины bee-box

Запустим сканирование через Nmap и сохраним в файл на рабочем столе.
Выполнение команды приведено на рисунке 8.

```

(nikita@kali)-[~]
└─$ sudo nmap -A --reason 172.20.10.2 -oX /home/nikita/Desktop/scan_bee.xml
[sudo] password for nikita:
Starting Nmap 7.92 ( https://nmap.org ) at 2022-07-13 03:25 EDT
Nmap scan report for 172.20.10.2
Host is up, received arp-response (0.00028s latency).
Not shown: 983 closed tcp ports (reset)
PORT      STATE SERVICE      REASON          VERSION
21/tcp    open  ftp          syn-ack ttl 64 ProFTPD 1.3.1
|_ ftp-anon: Anonymous FTP login allowed (FTP code 230)
|_ -rw-rw-r-- 1 root www-data 543803 Nov 2 2014 Iron_Man.pdf
|_ -rw-rw-r-- 1 root www-data 462949 Nov 2 2014 Terminator_Salvation.pdf
|_ -rw-rw-r-- 1 root www-data 544600 Nov 2 2014 The_Amazing_Spider-Man.pdf
|_ -rw-rw-r-- 1 root www-data 526187 Nov 2 2014 The_Cabin_in_the_Woods.pdf
|_ -rw-rw-r-- 1 root www-data 756522 Nov 2 2014 The_Dark_Knight_Rises.pdf
|_ -rw-rw-r-- 1 root www-data 618117 Nov 2 2014 The_Incredible_Hulk.pdf
|_ -rw-rw-r-- 1 root www-data 5010042 Nov 2 2014 bWAPP_intro.pdf
22/tcp    open  ssh          syn-ack ttl 64 OpenSSH 4.7p1 Debian 8ubuntu1 (protocol 2.0)
|_ ssh-hostkey:
|_ 1024 45:a4:66:ec:3a:ba:97:f8:3e:1a:ba:1c:24:68:22:e8 (DSA)
|_ 2048 63:e7:c5:d1:8d:8a:94:02:36:6a:d7:d2:75:e9:8b:ce (RSA)
25/tcp    open  smtp         syn-ack ttl 64 Postfix smtpd
|_ _smtp-commands: bee-box, PIPELINING, SIZE 1024000, VRFY, ETRN, STARTTLS, ENHANCEDSTATUSCODES, 8BITMIME, DSN
|_ ssly2:

```

Рисунок 8—Результат сканирования Nmap-ом bee-box-а

Заметим, что Nmap выдает информацию об открытом 21 порте с сервисом ftp⁵ с версией. Перейдем к работе с Metasploit. Для начала скачаем ее, затем инициализируем базу данных Metasploit PostgreSQL и запустим консоль (см. рисунок 9, 10).

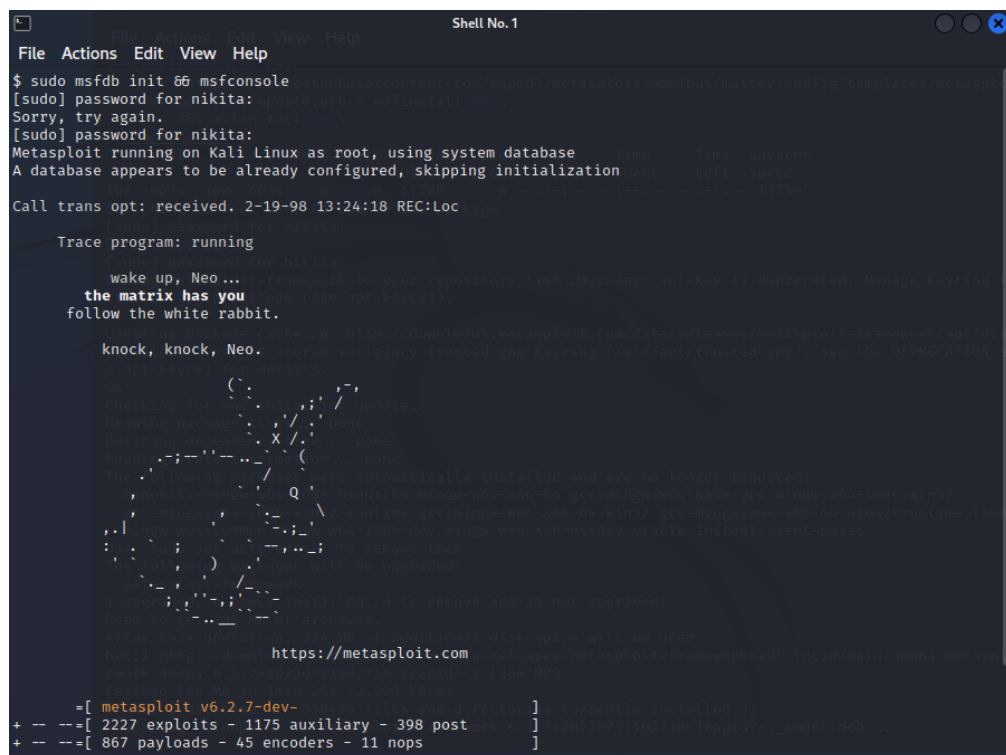
```

(nikita@kali)-[~]
└─$ curl https://raw.githubusercontent.com/rapid7/metasploit-omnibus/master/config/templates/metasploit-frame
work-wrappers/msfupdate.erb > msfinstall 66 \
  chmod 755 msfinstall 66 \
  ./msfinstall
% Total      % Received % Xferd Average Speed Time Time Time Current
           Dload Upload Total Spent Left Speed
100 6034 100 6034 0 0 11700 0 --:--:-- --:--:-- --:--:-- 11739
Switching to root user to update the package
[sudo] password for nikita: matrix has you
Sorry, try again.
[sudo] password for nikita:
Adding metasploit-framework to your repository list..Warning: apt-key is deprecated. Manage keyring files in
trusted.gpg.d instead (see apt-key(8)).
OK

```

Рисунок 9—Скачивание фреймворка с гита

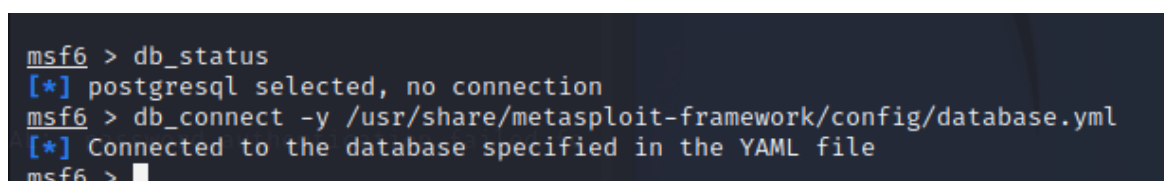
⁵ FTP — протокол передачи файлов по сети



```
File Actions Edit View Help
$ sudo msfdb init 56 msfconsole
[sudo] password for nikita:
Sorry, try again.
[sudo] password for nikita:
Metasploit running on Kali Linux as root, using system database
A database appears to be already configured, skipping initialization
Call trans opt: received. 2-19-98 13:24:18 REC:Loc
Trace program: running
wake up, Neo...
the matrix has you
follow the white rabbit.
knock, knock, Neo.
https://metasploit.com
+ --=[ metasploit v6.2.7-dev-
+ --=[ 2227 exploits - 1175 auxiliary - 398 post
+ --=[ 867 payloads - 45 encoders - 11 nops
```

Рисунок 10-Запуск консоли Metasploit и создание базы данных

Теперь подключим заранее созданную базу данных к фреймворку, что можно увидеть на рисунке 11.



```
msf6 > db_status
[*] postgresql selected, no connection
msf6 > db_connect -y /usr/share/metasploit-framework/config/database.yml
[*] Connected to the database specified in the YAML file
msf6 >
```

Рисунок 11-Проверка и подключение базы данных

Загрузим в базу данных наш скан от Nmap, далее посмотрим какие сервисы и хосты лежат в базе данных Metasploit. На рисунках 12 и 13 видно, что мы успешно загрузили скан и проверили его содержимое.


```
msf6 > db_import /home/nikita/Desktop/scan_bee.xml
[*] Importing 'Nmap XML' data
[*] Import: Parsing with 'Nokogiri v1.13.6'
[*] Importing host 172.20.10.2
[*] Successfully imported /home/nikita/Desktop/scan_bee.xml
msf6 > hosts
```

address	mac	name	os_name	os_flavor	os_sp	purpose	info	comments
172.20.10.2	08:00:27:d2:3e:98		Linux		2.6.X	server		

Рисунок 12–Импортирование результатов в базу данных и просмотр содержимого

```
msf6 > services
```

host	port	proto	name	state	info
172.20.10.2	21	tcp	ftp	open	ProFTPD 1.3.1
172.20.10.2	22	tcp	ssh	open	OpenSSH 4.7p1 Debian 8ubuntu1 protocol 2.0
172.20.10.2	25	tcp	smtp	open	Postfix smtpd
172.20.10.2	80	tcp	http	open	Apache httpd 2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4 -2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g
172.20.10.2	139	tcp	netbios-ssn	open	Samba smbd 3.X - 4.X workgroup: ITSECGAMES
172.20.10.2	443	tcp	ssl/http	open	Apache httpd 2.2.8 (Ubuntu) DAV/2 mod_fastcgi/2.4.6 PHP/5.2.4 -2ubuntu5 with Suhosin-Patch mod_ssl/2.2.8 OpenSSL/0.9.8g
172.20.10.2	445	tcp	netbios-ssn	open	Samba smbd 3.0.28a workgroup: ITSECGAMES
172.20.10.2	512	tcp	exec	open	netkit-rsh rshd
172.20.10.2	513	tcp	login	open	
172.20.10.2	514	tcp	shell	open	
172.20.10.2	666	tcp	doom	open	
172.20.10.2	3306	tcp	mysql	open	MySQL 5.0.96-0ubuntu3
172.20.10.2	5901	tcp	vnc	open	VNC protocol 3.8
172.20.10.2	6001	tcp	x11	open	access denied
172.20.10.2	8080	tcp	http	open	nginx 1.4.0
172.20.10.2	8443	tcp	ssl/http	open	nginx 1.4.0
172.20.10.2	9080	tcp	http	open	lighttpd 1.4.19

Рисунок 13–Проверка и подключение базы данных

Посмотрим на базу данных уязвимостей связанных с ProFTPD⁶. Результат показан на рисунке 14.

```
msf6 > search type:exploit proftpd
```

#	Name	Disclosure Date	Rank	Check	Description
0	exploit/linux/misc/netsupport_manager_agent	2011-01-08	average	No	NetSupport Manager Agent Remote Buffer Overflow
1	exploit/linux/ftp/proftpd_sreplace	2006-11-26	great	Yes	ProFTPD 1.2 - 1.3.0 sreplace Buffer Overflow (Linux)
2	exploit/freebsd/ftp/proftpd_telnet_iac	2010-11-01	great	Yes	ProFTPD 1.3.2rc3 - 1.3.3b Telnet IAC Buffer Overflow (FreeBSD)
3	exploit/linux/ftp/proftpd_telnet_iac	2010-11-01	great	Yes	ProFTPD 1.3.2rc3 - 1.3.3b Telnet IAC Buffer Overflow (Linux)
4	exploit/unix/ftp/proftpd_modcopy_exec	2015-04-22	excellent	Yes	ProFTPD 1.3.5 Mod_Copy Command Execution
5	exploit/unix/ftp/proftpd_133c_backdoor	2010-12-02	excellent	No	ProFTPD-1.3.3c Backdoor Command Execution

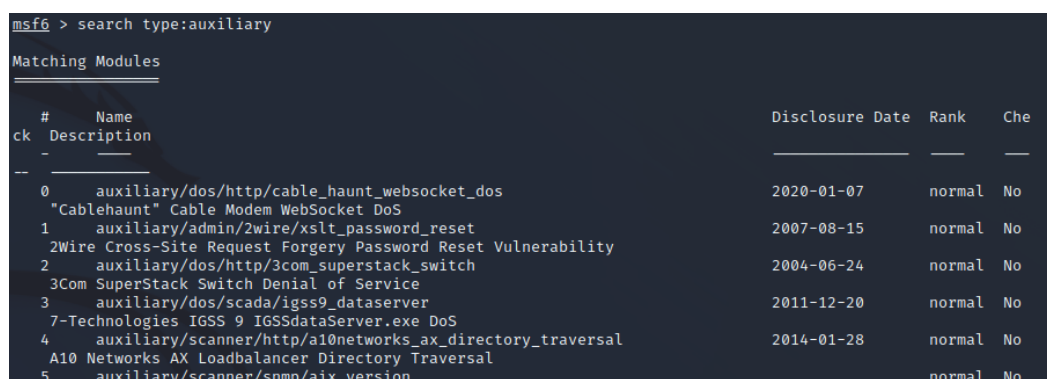
Рисунок 14–список уязвимостей

⁶ ProFTPD - Программное обеспечение FTP-сервера под лицензией GPL с широкими возможностями настройки

Мы видим огромное количество уязвимостей связанных с ProFTPD, но мы не нашли нашу версию. Но понимание, что это ПО имеет большое количество уязвимостей, включая и более новые версии, дает нам повод продолжать поиски.

Стоит отметить, что Metasploit имеет встроенный Nmap и мы могли бы не импортировать результаты скана в базу данных, если бы пользовались интегрированным Nmap-ом. Однако мы уже заметили, что его оказалось мало для полноценного анализа нашей машины на уязвимости.

Перейдем к инструментам Metasploit. Metasploit обладает огромным количеством встроенных инструментов и сканнеров, которые необходимы для тестов на проникновение, что можно видеть на рисунке 15.



```
msf6 > search type:auxiliary
```

Matching Modules				
#	Name	Disclosure Date	Rank	Che
ck	Description			
0	auxiliary/dos/http/cable_haunt_websocket_dos "Cablehaunt" Cable Modem WebSocket DoS	2020-01-07	normal	No
1	auxiliary/admin/2wire/xslt_password_reset 2Wire Cross-Site Request Forgery Password Reset Vulnerability	2007-08-15	normal	No
2	auxiliary/dos/http/3com_superstack_switch 3Com SuperStack Switch Denial of Service	2004-06-24	normal	No
3	auxiliary/dos/scada/igss9_dataserver 7-Technologies IGSS 9 IGSSdataServer.exe DoS	2011-12-20	normal	No
4	auxiliary/scanner/http/a10networks_ax_directory_traversal A10 Networks AX Loadbalancer Directory Traversal	2014-01-28	normal	No
5	auxiliary/scanner/snmp/aix_version		normal	No

Рисунок 15–Вывод вспомогательных программ и скриптов

Перейдем от общих материалов к нашим для продолжения поиска уязвимостей открыто порта. Уязвимости ПО приведены на рисунке 16.

```
msf6 > search type:exploit proftpd
```

Matching Modules						Письма на тему	
#	Name	Disclosure Date	Rank	Check	Description		
0	exploit/linux/misc/netsupport_manager_agent	2011-01-08	average	No	NetSupport Manager Agen		
1	exploit/linux/ftp/proftpd_sreplace	2006-11-26	great	Yes	ProFTPD 1.2 - 1.3.0 sre		
2	exploit/freebsd/ftp/proftpd_telnet_iac	2010-11-01	great	Yes	ProFTPD 1.3.2rc3 - 1.3.		
3	exploit/linux/ftp/proftpd_telnet_iac	2010-11-01	great	Yes	ProFTPD 1.3.2rc3 - 1.3.		
4	exploit/unix/ftp/proftpd_modcopy_exec	2015-04-22	excellent	Yes	ProFTPD 1.3.5 Mod_Copy		
5	exploit/unix/ftp/proftpd_133c_backdoor	2010-12-02	excellent	No	ProFTPD-1.3.3c Backdoor		

Рисунок 16–Вывод инструментов для нашего ПО

Использование всех инструментов не дало результатов. Подойдем с другой стороны: Metasploit также имеет список exploit-ов и через метод show targets мы можем смотреть к каким версиям ПО они применимы. Результат выполнения команды show targets показан на рисунке 17.

```
msf6 auxiliary(admin/http/manageengine_pmp_privesc) > use exploit/linux/ftp/proftpd_telnet_iac
[*] No payload configured, defaulting to linux/x86/meterpreter/reverse_tcp
msf6 exploit(linux/ftp/proftpd_telnet_iac) > show targets
```

Exploit targets:	
Id	Name
0	Automatic Targeting
1	Debug
2	ProFTPD 1.3.3a Server (Debian) - Squeeze Beta1
3	ProFTPD 1_3_3a Server (Debian) - Squeeze Beta1 (Debug)

Рисунок 17–Возможность применения exploit-a

Перебор всех exploit-ов также не дал результатов для нашей версии. Однако мы постоянно встречаем соседние версии программного обеспечения.

Проверим нашу гипотезу о уязвимости с помощью базы данных уязвимостей CVE (см. рисунок 18).

6,8
CVSSv2

CVE-2008-4242

Опубликовано: 25.09.2008 Обновлено: 08.08.2017

CVSS v2 Базовая оценка: 6,8 | Оценка воздействия: 6,4 | Оценка эксплуатационной пригодности: 8,6

VMscore: 605

Вектор: AV:N/AC:M/Au:N/C:P/I:P/A:P

[Подписаться на проект Proftpd](#)

Сводка уязвимостей

ProFTPD 1.3.1 интерпретирует длинные команды от FTP-клиента как несколько команд, что позволяет удаленным злоумышленникам проводить атаки с подделкой межсайтовых запросов (CSRF) и выполнять произвольные FTP-команды с помощью длинного URI ftp://, который использует существующий сеанс из реализации FTP-клиента в веб-браузере.

Рисунок 18—Уязвимость из CVE

Таким образом, наше предположение оказалось правдой. Также стоит отметить, что по ходу прохождения практики часто встречались понятия CVE, CVSS, с которыми мы работали ранее (в пунктах 2 и 3), из чего можно сделать вывод о востребованности и актуальности полученных знаний и о удовлетворенностью полученных результатов.

Попробуем все же найти уязвимости бее-бох-а. Для этого воспользуемся WMAP⁷. Он автоматизирует использование инструментов Metasploit. Работа сканнера и его скачивание показано на рисунках 19, 20, 21.

```
msf6 > load wmap
[*] Successfully loaded plugin: wmap
msf6 > wmap_sites -a 172.20.10.2
[*] Site created.
```

Рисунок 19—Скачивание сканера и добавление нашего IP в него

⁷ WMAP — это многофункциональный сканер уязвимостей веб-приложений
Москва, 2022

```

msf6 > wmap_run -e
[*] Using ALL wmap enabled modules.
[-] NO WMAP NODES DEFINED. Executing local modules
[-] Targets have not been selected.
msf6 > wmap_targets -t http://172.20.10.2
msf6 > wmap_run -e
[*] Using ALL wmap enabled modules.
[-] NO WMAP NODES DEFINED. Executing local modules
[*] Testing target:
[*]   Site: 172.20.10.2 (172.20.10.2)
[*]   Port: 80 SSL: false

[*] Testing started. 2022-07-13 05:07:03 -0400
[*] Loading wmap modules ...
[*] 40 wmap enabled modules loaded.

```

Рисунок 20—Запуск скрипта

```

[*] Done.
msf6 > wmap_vulns -l
[*] + [172.20.10.2] (172.20.10.2): directory /doc/
[*]   directory Directory found.
[*]   GET Res code: 403
[*] + [172.20.10.2] (172.20.10.2): directory /icons/
[*]   directory Directory found.
[*]   GET Res code: 200
[*] + [172.20.10.2] (172.20.10.2): directory /phpmyadmin/
[*]   directory Directory found.
[*]   GET Res code: 200
[*] + [172.20.10.2] (172.20.10.2): directory /webdav/
[*]   directory Directory found.
[*]   GET Res code: 200
[*] + [172.20.10.2] (172.20.10.2): file /index.bak
[*]   file File found.
[*]   GET Res code: 404
[*] + [172.20.10.2] (172.20.10.2): file /index.html
[*]   file File found.
[*]   GET Res code: 404
[*] + [172.20.10.2] (172.20.10.2): file /index
[*]   file File found.
[*]   GET Res code: 404
[*] + [172.20.10.2] (172.20.10.2): file /phpmyadmin
[*]   file File found.
[*]   GET Res code: 301
[*] + [172.20.10.2] (172.20.10.2): file /webdav
[*]   file File found.
[*]   GET Res code: 301
msf6 >

```

Рисунок 21—Результаты сканирование

Отметим, что тут был иной подход, модули просматривали нашу машину как веб-сервис и искали наиболее распространенные относительные URL-адрес страницы. Все наши предыдущие подходы основывались на проверке портов.

Проверим нашу базу данных на внесенные изменение после запуска WMAP (см. рисунок 22).

Vulnerabilities			
Timestamp	Host	Name	References
2022-07-13 09:07:24 UTC	172.20.10.2	HTTP Trace Method Allowed	CVE-2005-3398,CVE-2005-3498,OSVDB-877,BID-11604,BID-9506,BID-9561

Рисунок 22—Найденные уязвимости

Видим, что сканнер нашел уязвимость и добавил ее. Посмотрим ее в базе CVE [7]. Имеем: “Конфигурация веб-сервера по умолчанию для консоли управления Solaris (SMC) в Solaris 8, 9 и 10 включает метод HTTP TRACE, который может позволить удаленным злоумышленникам получать конфиденциальную информацию, такую как файлы cookie и данные проверки подлинности, из заголовков HTTP.”.

Стоит отметить, что использование данного сканера не только ускорило процесс перебора инструментов, но и помог достичь желаемого результата.