

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО
ОБРАЗОВАНИЯ**

**«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИНЖЕНЕРНЫХ
ТЕХНОЛОГИЙ»**

**Факультет управления и информатики в технологических системах
Кафедра информационной безопасности
Направление подготовки (специальность) 10.05.03 Информационная
безопасность автоматизированных систем**

**Отчет
по лабораторной работе №1**

Выполнил студент гр. УБ-32

Потапов Роман Михайлович

Номер зачётной книжки:

100503_237196

Проверил:

профессор каф. Хвостов В. А.
(должность, ф.и.о)

(оценка)

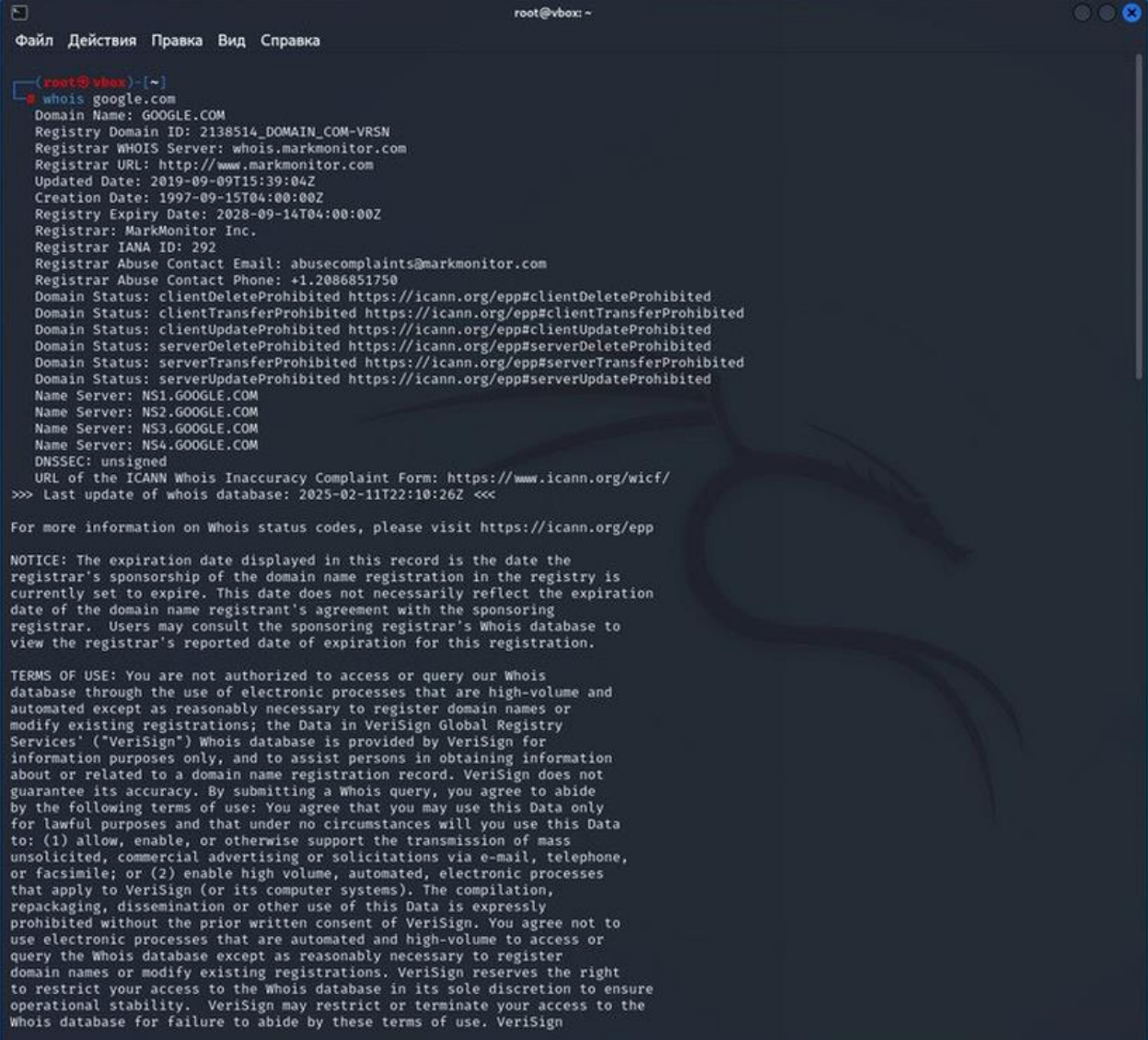
(подпись)

(дата)

Воронеж – 2025

Цель работы: Ознакомиться с методами сбора информации о целевых домене по открытым источникам с использованием специальных инструментов. Собрать информацию о целевом домене с использованием общедоступных ресурсов, которые можно применять для сбора информации о целевом домене.

Ход работы:



```
root@vbox: ~  
Файл Действия Правка Вид Справка  
root@vbox: ~  
# whois google.com  
Domain Name: GOOGLE.COM  
Registry Domain ID: 2138514_DOMAIN_COM-VRSN  
Registrar WHOIS Server: whois.markmonitor.com  
Registrar URL: http://www.markmonitor.com  
Updated Date: 2019-09-09T15:39:04Z  
Creation Date: 1997-09-15T04:00:00Z  
Registry Expiry Date: 2028-09-14T04:00:00Z  
Registrar: MarkMonitor Inc.  
Registrar IANA ID: 292  
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com  
Registrar Abuse Contact Phone: +1.2086851750  
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited  
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited  
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited  
Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited  
Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited  
Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited  
Name Server: NS1.GOOGLE.COM  
Name Server: NS2.GOOGLE.COM  
Name Server: NS3.GOOGLE.COM  
Name Server: NS4.GOOGLE.COM  
DNSSEC: unsigned  
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/  
>>> Last update of whois database: 2025-02-11T22:10:26Z <<<  
  
For more information on Whois status codes, please visit https://icann.org/epp  
  
NOTICE: The expiration date displayed in this record is the date the  
registrar's sponsorship of the domain name registration in the registry is  
currently set to expire. This date does not necessarily reflect the expiration  
date of the domain name registrant's agreement with the sponsoring  
registrar. Users may consult the sponsoring registrar's Whois database to  
view the registrar's reported date of expiration for this registration.  
  
TERMS OF USE: You are not authorized to access or query our Whois  
database through the use of electronic processes that are high-volume and  
automated except as reasonably necessary to register domain names or  
modify existing registrations; the Data in VeriSign Global Registry  
Services' ("VeriSign") Whois database is provided by VeriSign for  
information purposes only, and to assist persons in obtaining information  
about or related to a domain name registration record. VeriSign does not  
guarantee its accuracy. By submitting a Whois query, you agree to abide  
by the following terms of use: You agree that you may use this Data only  
for lawful purposes and that under no circumstances will you use this Data  
to: (1) allow, enable, or otherwise support the transmission of mass  
unsolicited, commercial advertising or solicitations via e-mail, telephone,  
or facsimile; or (2) enable high volume, automated, electronic processes  
that apply to VeriSign (or its computer systems). The compilation,  
repackaging, dissemination or other use of this Data is expressly  
prohibited without the prior written consent of VeriSign. You agree not to  
use electronic processes that are automated and high-volume to access or  
query the Whois database except as reasonably necessary to register  
domain names or modify existing registrations. VeriSign reserves the right  
to restrict your access to the Whois database in its sole discretion to ensure  
operational stability. VeriSign may restrict or terminate your access to the  
Whois database for failure to abide by these terms of use. VeriSign
```

Рисунок 1 – Полный вывод команды whois

```

(root@vbox)-[~]
# whois google.com
Domain Name: GOOGLE.COM
Registry Domain ID: 2138514_DOMAIN_COM-VRSN
Registrar WHOIS Server: whois.markmonitor.com
Registrar URL: http://www.markmonitor.com
Updated Date: 2019-09-09T15:39:04Z
Creation Date: 1997-09-15T04:00:00Z
Registry Expiry Date: 2028-09-14T04:00:00Z
Registrar: MarkMonitor Inc.
Registrar IANA ID: 292
Registrar Abuse Contact Email: abusecomplaints@markmonitor.com
Registrar Abuse Contact Phone: +1.2086851750
Domain Status: clientDeleteProhibited https://icann.org/epp#clientDeleteProhibited
Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited
Domain Status: clientUpdateProhibited https://icann.org/epp#clientUpdateProhibited
Domain Status: serverDeleteProhibited https://icann.org/epp#serverDeleteProhibited
Domain Status: serverTransferProhibited https://icann.org/epp#serverTransferProhibited
Domain Status: serverUpdateProhibited https://icann.org/epp#serverUpdateProhibited
Name Server: NS1.GOOGLE.COM
Name Server: NS2.GOOGLE.COM
Name Server: NS3.GOOGLE.COM
Name Server: NS4.GOOGLE.COM
DNSSEC: unsigned
URL of the ICANN Whois Inaccuracy Complaint Form: https://www.icann.org/wicf/
>>> Last update of whois database: 2025-02-11T22:10:26Z <<<

```

Рисунок 2 – Первый блок вывода команды whois

```

(root@vbox)-[~]
# host google.com
google.com has address 172.217.23.206
google.com has IPv6 address 2a00:1450:400e:805::200e
google.com mail is handled by 10 smtp.google.com.

```

Рисунок 3 – Вывод команды host

```

(root@vbox)-[~]
# host 172.217.23.206
206.23.217.172.in-addr.arpa domain name pointer prg03s05-in-f206.1e100.net.
206.23.217.172.in-addr.arpa domain name pointer ams16s37-in-f14.1e100.net.
206.23.217.172.in-addr.arpa domain name pointer prg03s05-in-f14.1e100.net.

```

Рисунок 4 – Метод обратного просмотра

```

(root@vbox)-[~]
# dig google.com

; <<>> DiG 9.20.2-1-Debian <<>> google.com
;; global options: +cmd
;; Got answer:
;; ->HEADER<- opcode: QUERY, status: NOERROR, id: 22431
;; flags: qr ra; QUERY: 1, ANSWER: 1, AUTHORITY: 0, ADDITIONAL: 0

;; QUESTION SECTION:
;google.com.                IN      A

;; ANSWER SECTION:
google.com.                 0       IN      A      172.217.23.206

;; Query time: 87 msec
;; SERVER: 10.0.2.3#53(10.0.2.3) (UDP)
;; WHEN: Wed Feb 12 01:20:13 MSK 2025
;; MSG SIZE rcvd: 44

```

Рисунок 5 – Вывод команды dig

```

(root@vbox)-[~]
# dmitry
DeePMagic Information Gathering Tool
"There be some deep magic going on"

Usage: dmitry [-winsepfb] [-t 0-9] [-o %host.txt] host
  -o      Save output to %host.txt or to file specified by -o file
  -i      Perform a whois lookup on the IP address of a host
  -w      Perform a whois lookup on the domain name of a host
  -n      Retrieve Netcraft.com information on a host
  -s      Perform a search for possible subdomains
  -e      Perform a search for possible email addresses
  -p      Perform a TCP port scan on a host
* -f      Perform a TCP port scan on a host showing output reporting filtered ports
* -b      Read in the banner received from the scanned port
* -t 0-9  Set the TTL in seconds when scanning a TCP port ( Default 2 )
*Requires the -p flagged to be passed

```

Рисунок 6 – Запуск dmitry


```

(root@vbox)-[~]
# dmitry -iwnse google.com
Deepmagic Information Gathering Tool
"There be some deep magic going on"

HostIP:172.217.23.206
HostName:google.com

Gathered Inet-whois information for 172.217.23.206

inetnum: 172.216.0.0 - 172.240.255.255
netname: NON-RIPE-NCC-MANAGED-ADDRESS-BLOCK
descr: IPv4 address block not managed by the RIPE NCC
remarks:
remarks: For registration information,
remarks: you can consult the following sources:
remarks: IANA
s: http://www.iana.org/assignments/ipv4-address-space
remarks: http://www.iana.org/assignments/iana-ipv4-special-registry
remarks: http://www.iana.org/assignments/ipv4-recovered-address-space
remarks: AFRINIC (Africa)
remarks: http://www.afrinic.net/ whois.afrinic.net
remarks: APNIC (Asia Pacific)
remarks: http://www.apnic.net/ whois.apnic.net
remarks: ARIN (Northern America)
hois.arin.net
remarks: LACNIC (Latin America and the Carribean)
remarks: http://www.lacnic.net/ whois.lacnic.net
remarks:
remarks: EU # Country is really world wide
admin-c: IANA1-RIPE
tech-c: IANA1-RIPE
status: ALLOCATED UNSPECIFIED
mnt-by: RIPE-NCC-HM-MNT
created: 2022-06-22T14:31:59Z
last-modified: 2022-06-22T14:31:59Z
source: RIPE
Internet Assigned Numbers Authority
address: see http://www.iana.org.
admin-c: IANA1-RIPE
tech-c: IANA1-RIPE
nic-hdl: IANA1-RIPE
remarks: For more information on IANA services
remarks: go to IANA web site at http://www.iana.org.
mnt-by: RIPE-NCC-MNT
created: 1970-01-01T00:00:00Z
last-modified: 2001-09-22T09:31:27Z
source: RIPE # Filtered

```

Рисунок 7 – Полный вывод команды dmitry

```

(root@vbox)-[~]
# dmitry -iwnse google.com
Deepmagic Information Gathering Tool
"There be some deep magic going on"

HostIP:172.217.23.206
HostName:google.com

Gathered Inet-whois information for 172.217.23.206

inetnum: 172.216.0.0 - 172.240.255.255
netname: NON-RIPE-NCC-MANAGED-ADDRESS-BLOCK
descr: IPv4 address block not managed by the RIPE NCC

```

Рисунок 8 – Первый блок в выводе команды dmitry

```
(root@vbox)-[~]
# dmitry -p google.com -f -b
Deepmagic Information Gathering Tool
"There be some deep magic going on"

HostIP:172.217.23.206
HostName:google.com

Gathered TCP Port information for 172.217.23.206

```

Port	State
1/tcp	open

```
zsh: segmentation fault  dmitry -p google.com -f -b
```

Рисунок 9 – Сканирование портов с использованием dmitry