

Оглавление

Пассивный сбор информации о цели	2
Служба регистрации интернет услуг	2
Пример использования Network service based	3
Пример использования Name service based	6
Служба доменных имен	8
Dig	8
Nslookup	9
Почтовая служба	15
SMTP заголовки	16
Анализ фактических имен, используемых для определения каждого сетевого узла или службы.....	19
Фактический анализ сайта	20
robots.txt.....	21
Поисковые системы.....	21
Shodan	22
Vulners	27
Анализ SSL сертификатов	28
Служба Поддержки.....	34

4.2 Пассивный сбор информации о цели

В пентесте веб-приложений этап сбора информации, будь то пассивный или активный, а также анализ этой информации, является ключевым. Информация – самое сильное оружие. Ее не может быть много. Чем больше информации вы сможете собрать, чем лучше вы сможете ее проанализировать - тем эффективней будет ваш тест на проникновение.

Особенность пассивного сбора информации заключается в том, что при сборе информации у цели практически нет возможности отследить атакуемого. Другими словами, это сбор общедоступной информации.

С помощью пассивного сбора можно собрать такую информацию как: информация об организации, информацию о сотрудниках, приблизительное расположение внешних узлов сети и их роль, и так далее.

Для пассивного сбора информации можно выделить ряд основных ресурсов, которые помогут нам:

- Служба регистрации интернет услуг;
- Служба доменных имен;
- Почтовая служба;
- Анализ фактических имен, используемых для определения каждого сетевого узла или службы;
- Фактический анализ сайта;
- Поисковые системы.

Служба регистрации интернет услуг

Что бы получить доступ к сетевым ресурсам необходимо иметь IP адрес, который бывает двух видов: IPv6 и IPv4. С записью вида xxx.xxx.xxx.xxx, где xxx – число в диапазоне от 0 до 255, неудобно работать, поэтому придумали службы, которые связывают IP адрес с уникальным доменным именем. Например: 104.25.5.14 – codeby.net

Регистрация IP адресов и доменных имен регулируется на международном уровне, и для нормального управления всем этим

организации, которые хотят зарегистрировать свой сетевой ресурс, должны предоставлять административные данные. Например, фактические имена, адреса и контактные данные. Эта информация многим необходима, и получить ее может каждый.

Существует 4 региональных реестра, которые разделяют между собой ответственность по работе всей этой системы:

- APNIC – азиатско-тихоокеанский регион;
- ARIN – американский регион;
- LACNIC – латинская Америка и Карибы;
- RIPE NCC – Европа.

Есть ресурс, который называется WHOIS. Он предоставляет услуги по поиску информации в различных реестрах, описанных выше.

WHOIS сервисы делятся на 2 вида: *Network service based* и *Name service based*. Различие заключается лишь в том, что один уделяет больше внимания сетевой части, а второй доменному имени.

Пример использования Network service based

Пусть есть сайт `example.net`. После определения IP адреса выясняем, что подсеть находится в Чехии. Значит нужно использовать реестр RIPE NCC. Далее пользуемся консольной утилитой `whois`.

Результат запроса `whois -h whois.ripe.net 77.78.xxx.xxx`:

```
% This is the RIPE Database query service.
% The objects are in RPSL format.
%
% The RIPE Database is subject to Terms and Conditions.
% See http://www.ripe.net/db/support/db-terms-conditions.pdf
% Note: this output has been filtered.

% To receive output for a database update, use the "-B" flag.
% Information related to '77.78.xxx.64 - 77.78.xxx.95'

% Abuse contact for '77.78.xxx.64 - 77.78.xxx.95' is 'abuse@casablanca.cz'
```

inetnum: 77.78.xxx.64 - 77.78.xxx.95
netname: HakenAdam-CZ
descr: Adam Haken
country: CZ
admin-c: CASA3-RIPE
tech-c: CASA3-RIPE
status: ASSIGNED PA
mnt-by: CASABLANCA-RIPE-MNT
created: 2009-08-03T14:12:15Z
last-modified: 2009-08-03T14:12:15Z
source: RIPE

role: Casablanca INT RIPE manager
address: Casablanca INT
address: Vinohradska 184, Prague 3 - xxx 52
address: Czech republic
phone: +420 270 000 xxx
fax-no: +420 270 000 xxx
abuse-mailbox: abuse@casablanca.cz
admin-c: JH1771-RIPE
tech-c: JH1771-RIPE
nic-hdl: CASA3-RIPE
created: 2005-09-05T10:42:10Z
last-modified: 2015-07-03T11:19:49Z
source: RIPE # Filtered
mnt-by: CASABLANCA-CORE-MNT

% Information related to '77.78.xxx.0/24AS156xx'

route: 77.78.xxx.0/24
descr: Casablanca INT prefix fraction
origin: AS156xx
mnt-by: CASABLANCA-CORE-MNT
created: 2017-06-30T09:38:49Z
last-modified: 2017-06-30T09:38:49Z
source: RIPE

% This query was served by the RIPE Database Query Service version 1.92.5
(HEREFORD)

Получили много полезной информации: диапазон 77.78.xxx.64 – 77.78.xxx.95 управляется HakenAdam-CZ, находится в Кособланке и имеет бизнес роль Casablanca INT RIPE manager. Также были представлены контактные данные address: Casablanca INT, address: Vinohradska xxx, Prague 3 - xxx 52, address: Czech Republic, phone: +420 270 000 xxx fax-no: +420 270 000 xxx, abuse- mailbox: abuse@casablanca.cz

Идем дальше и проверяем: `whois -h whois.ripe.net CASABLANCA-CORE-MNT`

```
% This is the RIPE Database query service.
% The objects are in RPSL format.
%
% The RIPE Database is subject to Terms and Conditions.
% See http://www.ripe.net/db/support/db-terms-conditions.pdf

% Note: this output has been filtered.
% To receive output for a database update, use the "-B" flag.

% Information related to 'CASABLANCA-CORE-MNT'

mntner: CASABLANCA-CORE-MNT
descr: Core object MNT for Casablanca
admin-c: CASA3-RIPE
admin-c: JH1771-RIPE
tech-c: CASA3-RIPE
tech-c: JH1771-RIPE
auth: PGPKEY-64A611B0
auth: PGPKEY-B0C07729
auth: SSO # Filtered
mnt-by: CASABLANCA-CORE-MNT
mnt-by: JH1771-RIPE-MNT
created: 2014-04-09T08:20:40Z
last-modified: 2017-11-13T15:54:21Z
source: RIPE # Filtered

role: Casablanca INT RIPE manager
address: Casablanca INT
address: Vinohradska 184, Prague 3 - xxx xxx
```

address: Czech republic
phone: +420 270 000 xxx
fax-no: +420 270 000 xxx
abuse-mailbox: abuse@casablanca.cz
admin-c: JH1771-RIPE
tech-c: JH1771-RIPE
nic-hdl: CASA3-RIPE
created: 2005-09-05T10:42:10Z
last-modified: 2015-07-03T11:19:49Z
source: RIPE # Filtered
mnt-by: CASABLANCA-CORE-MNT

person: Jan Hampl
address: Casablanca INT s.r.o.
address: Vinohradská xxx
address: xxx 52 Praha 3
address: The Czech Republic
phone: +420 270 000 xxx
fax-no: +420 270 000 xxx
nic-hdl: JH1771-RIPE
created: 2003-02-28T14:37:38Z
last-modified: 2015-07-13T11:04:26Z
source: RIPE # Filtered
mnt-by: JH1771-RIPE-MNT
% This query was served by the RIPE Database Query Service version 1.92.5
(BLAARKOP)

Получаем человека, на которого зарегистрирован сетевой ресурс, его контакты и адрес.

Пример использования Name service based

Все тот же сайт. Проверим результат запроса по доменному имени командой: *whois example.com*

Domain Name: xxx.net
Registry Domain ID: 1763971xxx_DOMAIN_NET-VRSN
Registrar WHOIS Server: whois.regtons.com
Registrar URL: http://regtons.com

Updated Date: 2017-01-26T00:00:00Z
Creation Date: 2012-12-04T00:00:00Z
Registrar Registration Expiration Date: 2026-12-04T00:00:00Z
Registrar: GRANSY S.R.O D/B/A SUBREG.CZ
Registrar IANA ID: 150xxx
Registrar Abuse Contact Email: abuse@regtons.com
Registrar Abuse Contact Phone: +420.734463xxx
DD: 16xxx
Reseller:
Domain Status: clientDeleteProhibited <https://www.icann.org/eppxxx>
Domain Status: clientTransferProhibited <https://www.icann.org/eppxxx>
Domain Status: clientUpdateProhibited <https://www.icann.org/eppxxx>
Registrant Organization: Whois protection, this company does not own this domain name s.r.o..
Registrant State/Province:
Registrant Country: CZ
Registrant Email: webproxy@whoisprotection.domains
Admin Organization: Whois protection, this company does not own this domain name s.r.o..
Admin Email: webproxy@whoisprotection.domains
Tech Organization: Whois protection, this company does not own this domain name s.r.o..
Tech Email: webproxy@whoisprotection.domains
Name Server: ns.gransy.com
Name Server: ns2.gransy.com
Name Server: ns3.gransy.com
Name Server: ns4.gransy.com
Name Server: ns5.gransy.com
DNSSEC: unsigned
URL of the ICANN WHOIS Data Problem Reporting System:
<http://wdprs.internic.net/>
>>> Last update of WHOIS database: 2018-09-17T11:00:00Z <<<

Как видим, много информации можно подчерпнуть, используя данный метод.

Также, для получения этой информации, можно воспользоваться сторонними сервисами:

- ✓ whoer.net
- ✓ who.is
- ✓ whois.net

Служба доменных имен

Как описывалось ранее, доменные имена используются для того, чтобы человеку было проще запоминать адреса узлов в сети. Есть несколько реализаций службы DNS, но самая распространенная называется BIND. Учитывая особенности службы, запросы на получение DNS записей могут дать множество полезной информации.

Самой распространенной утилитой для работы с DNS является dig. Этот инструмент идет в комплекте с BIND и включает такие возможности как: получения IP адресов через доменное имя, получение доменного имени через IP адрес, получение версии DNS и т.д.

Так же популярной утилитой является nslookup, которая устанавливается в большинство операционных систем.

Возьмем цель из предыдущего примера и сравним работу утилит dig и nslookup.

Dig

```
; <<>> DiG 9.10.3-P4-Ubuntu <<>> xxx.net any
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 2281
;; flags: qr rd ra; QUERY: 1, ANSWER: 8, AUTHORITY: 0, ADDITIONAL: 1

;; OPT PSEUDOSECTION:
; EDNS: version: 0, flags;; udp: 1280

;; QUESTION SECTION:
;xxx.net. IN ANY

;; ANSWER SECTION:
```



```
xxx.net. 1624 IN SOA ns.gransy.com. root.gransy.com. 2014101056 86400
900 1209600 1800
xxx.net. 1624 IN NS ns.gransy.com.
xxx.net. 1624 IN NS ns2.gransy.com.
xxx.net. 1624 IN NS ns3.gransy.com.
xxx.net. 1624 IN NS ns4.gransy.com.
xxx.net. 1624 IN NS ns5.gransy.com.
xxx.net. 1624 IN A 77.78.109.83
xxx.net. 1624 IN MX 10 ws.zacatek.cz.
;; Query time: 54 msec
```

Nslookup

```
Server: 127.0.1.1
Address: 127.0.1.1#53

Non-authoritative answer:
xxx.net
origin = ns.gransy.com
mail addr = root.gransy.com
serial = 2014101056
refresh = 86400
retry = 900
expire = 1209600
minimum = 1800
xxx.net  nameserver = ns.gransy.com.
xxx.net  nameserver = ns2.gransy.com.
xxx.net  nameserver = ns3.gransy.com.
xxx.net  nameserver = ns4.gransy.com.
xxx.net  nameserver = ns5.gransy.com.
Name: xxx.net
Address: 77.78.109.83
xxx.net mail exchanger = 10 ws.zacatek.cz.
```

Authoritative answers can be found from:

В результате получили: несколько DNS серверов и 1 почтовый. Что такое ресурсная запись? (A, NS, MX, SOA ...)

A	Адресная запись; соответствие имени к адресу
MX	Адрес почтового шлюза домена состоит из приоритета и адреса узла. Чем выше цифра, тем ниже приоритет
NS	Адрес узла, отвечающий за доменную зону
PTR	Обратное соответствие адреса узла к имени
SOA	Указание на авторитетность информации
TXT	Запись произвольных двоичных данных

** Это не полный список.*

У DNS-сервера существует специальный метод, позволяющий передавать список информации о домене между первичными и вторичными серверами – Zone Transfer.

Если DNS-сервер был недостаточно хорошо настроен, то любой клиент может запросить и получить передачу зоны.

Рассмотрим на примере *zonetransfer.me*

dig @nsztm2.digi.ninja zonetransfer.me axfr

```
; <<>> DiG 9.10.3-P4-Ubuntu <<>> @nsztm2.digi.ninja zonetransfer.me axfr
; (1 server found)
;; global options: +cmd
zonetransfer.me. 7200 IN SOA nsztm1.digi.ninja. robin.digi.ninja. 2017103001
172800 900 1209600 3600
zonetransfer.me. 300 IN HINFO "Casio fx-700G" "Windows XP"
zonetransfer.me. 301 IN TXT "google-siteverification=
tyP28J7JAUHA9fw2sHXMgcCC0I6XBmmoVi04VIMewxA"
zonetransfer.me. 7200 IN MX 0 ASPMX.L.GOOGLE.COM.
zonetransfer.me. 7200 IN MX 10 ALT1.ASPMX.L.GOOGLE.COM.
zonetransfer.me. 7200 IN MX 10 ALT2.ASPMX.L.GOOGLE.COM.
zonetransfer.me. 7200 IN MX 20 ASPMX2.GOOGLEMAIL.COM.
zonetransfer.me. 7200 IN MX 20 ASPMX3.GOOGLEMAIL.COM.
zonetransfer.me. 7200 IN MX 20 ASPMX4.GOOGLEMAIL.COM.
zonetransfer.me. 7200 IN MX 20 ASPMX5.GOOGLEMAIL.COM.
zonetransfer.me. 7200 IN A 217.147.177.157
zonetransfer.me. 7200 IN NS nsztm1.digi.ninja.
```

```

zonetransfer.me. 7200 IN NS nsztm2.digi.ninja.
_sip._tcp.zonetransfer.me. 14000 IN SRV 0 0 5060 www.zonetransfer.me.
157.177.147.217.IN-ADDR.ARPA.zonetransfer.me.      7200      IN      PTR
www.zonetransfer.me.
asfdbauthdns.zonetransfer.me. 7900 IN AFSDB 1 asfdbbox.zonetransfer.me.
asfdbbox.zonetransfer.me. 7200 IN A 127.0.0.1
asfdbvolume.zonetransfer.me. 7800 IN AFSDB 1 asfdbbox.zonetransfer.me.
canberra-office.zonetransfer.me. 7200 IN A 202.14.81.230
cmdexec.zonetransfer.me. 300 IN TXT "; ls"
contact.zonetransfer.me. 2592000 IN TXT "Remember to call or email Pippa on
+44 123
4567890 or pippa@zonetransfer.me when making DNS changes"
dc-office.zonetransfer.me. 7200 IN A 143.228.181.132
deadbeef.zonetransfer.me. 7201 IN AAAAdead:beaf::
dr.zonetransfer.me. 300 IN LOC 53 20 56.558 N 1 38 33.526 W 0.00m 1m
10000m
10m
DZC.zonetransfer.me.7200 IN TXT "AbCdEfG"
email.zonetransfer.me. 2222 IN NAPTR 1 1 "P" "E2U+email" ""
email.zonetransfer.me.zonetransfer.me.
email.zonetransfer.me. 7200 IN A 74.125.206.26
home.zonetransfer.me. 7200 IN A 127.0.0.1
Info.zonetransfer.me. 7200 IN TXT "ZoneTransfer.me service provided by Robin
Wood -
robin@digi.ninja. See http://digi.ninja/projects/zonetransferme.php for more
information."
internal.zonetransfer.me. 300 IN NS intns1.zonetransfer.me.
internal.zonetransfer.me. 300 IN NS intns2.zonetransfer.me.
intns1.zonetransfer.me. 300 IN A 81.4.108.41
intns2.zonetransfer.me. 300 IN A 52.91.28.78
office.zonetransfer.me. 7200 IN A 4.23.39.254
ipv6actnow.org.zonetransfer.me. 7200 IN AAAA2001:67c:2e8:11::c100:1332
owa.zonetransfer.me. 7200 IN A 207.46.197.32
robinwood.zonetransfer.me. 302 IN TXT "Robin Wood"
rp.zonetransfer.me.      321      IN      RP      robin.zonetransfer.me.
robinwood.zonetransfer.me.
sip.zonetransfer.me.      3333      IN      NAPTR      2      3      "P"      "E2U+sip"
"!^.*$!sip:customerservice@
zonetransfer.me!" .

```

```
sqli.zonetransfer.me. 300 IN TXT "" or 1=1 --"
sshock.zonetransfer.me. 7200 IN TXT "() { :}; echo ShellShocked"
staging.zonetransfer.me. 7200 IN CNAME www.sydneypoperahouse.com.
alltcpportsopen.firewall.test.zonetransfer.me. 301 IN A 127.0.0.1
testing.zonetransfer.me. 301 IN CNAME www.zonetransfer.me.
vpn.zonetransfer.me. 4000 IN A 174.36.59.154
www.zonetransfer.me. 7200 IN A 217.147.177.157
xss.zonetransfer.me. 300 IN TXT ""<script>alert('Boo')</script>"
zonetransfer.me. 7200 IN SOA nsztm1.digi.ninja. robin.digi.ninja. 2017103001
172800 900 1209600 3600
;; Query time: 130 msec
;; SERVER: 52.91.28.78#53(52.91.28.78)
;; WHEN: Tue Sep 18 09:39:36 MSK 2018
;; XFR size: 48 records (messages 1, bytes 1878)
```

Результат на лицо. Большое количество информации, в которой можно найти слабое место в защите.

Также можно воспользоваться онлайн сервисами, например,

✓ hackertarget.com/zone-transfer

Так существует метод, отражающий новую информацию, которую не смогли показать предыдущие методы – реверсивный опрос DNS.

Осуществляется он следующим образом. Берется пул IP адресов выше и ниже IP адреса цели и производится обратный опрос DNS.

Приблизительный результат выглядит так:

```
107.xxx.xxx.18
107.xxx.xxx.19
107.xxx.xxx.20
107.xxx.xxx.21
107.xxx.xxx.22
107.xxx.xxx.23
107.xxx.xxx.24
107.xxx.xxx.25
107.xxx.xxx.26 test.nyc.ramnode.com.
```

107.xxx.xxx.27
107.xxx.xxx.28
107.xxx.xxx.29
107.xxx.xxx.30
107.xxx.xxx.31 radio.odong.co.
107.xxx.xxx.32 server.guiadabahia.com.br.
107.xxx.xxx.33 fujship.zeehostbox.com.
107.xxx.xxx.34 ny.lnbri.net.
107.xxx.xxx.35 mysql.doridian.net.
107.xxx.xxx.36
107.xxx.xxx.37 mx4.sctio.com.
107.xxx.xxx.38 anput.zeroground.net.
107.xxx.xxx.39 jbx.fixerme.com.
107.xxx.xxx.40
107.xxx.xxx.41
107.xxx.xxx.42 znc.tetralemma.faith.
107.xxx.xxx.43
107.xxx.xxx.44 shadow.apexirc.net.
107.xxx.xxx.45 webchat.apexirc.net.
107.xxx.xxx.46 sharetheguide.com.
107.xxx.xxx.47 vps.oneorzero.ca.
107.xxx.xxx.48 quoque.cf.
107.xxx.xxx.49 ns2.sentrynetworkgroup.net.
107.xxx.xxx.50 google.evagenna.com.
107.xxx.xxx.51
107.xxx.xxx.52 host0.dailynewsalerts.space.
107.xxx.xxx.53 kv3.com.
107.xxx.xxx.54 n04.sender.guru.
107.xxx.xxx.55
107.xxx.xxx.56 nyc2.ae97.net.
107.xxx.xxx.57
107.xxx.xxx.58
107.xxx.xxx.59
107.xxx.xxx.60 server.patienceprovidence.com.
107.xxx.xxx.61 ns1.viltr.com.
107.xxx.xxx.62
107.xxx.xxx.63
107.xxx.xxx.64 inspektech003.inspektech.com.
107.xxx.xxx.65 nyc.glownew.com.

```
107.xxx.xxx.66
107.xxx.xxx.67 bumbr.com.
107.xxx.xxx.68
107.xxx.xxx.69 server.danscartoons.com.
107.xxx.xxx.70
107.xxx.xxx.71 mail.solution-email.us.
107.xxx.xxx.72
107.xxx.xxx.73 ny2.steel-orchid.com.
107.xxx.xxx.74
107.xxx.xxx.75
107.xxx.xxx.76 voip.cryptohost.io.
107.xxx.xxx.77 x-r2-06.originaldata.info.
107.xxx.xxx.78 nyc1.tashfeen.com.
107.xxx.xxx.79
107.xxx.xxx.80
107.xxx.xxx.81
```

Там, где пусто означает, что у DNS нет записи для данного IP адреса.

Для воспроизведения данной методики предлагаю использовать следующий скрипт:

```
#!/bin/bash
1 NET=xxx.xxx
2 for i in $(seq x1 x2); do
3   for j in $(seq x1 x2); do
4     ADDR=${NET}.${i}.${j}
5     echo -e "${ADDR}\t$(dig -x ${ADDR} +short)"
6   done
7 done
```

Разберем по частям:

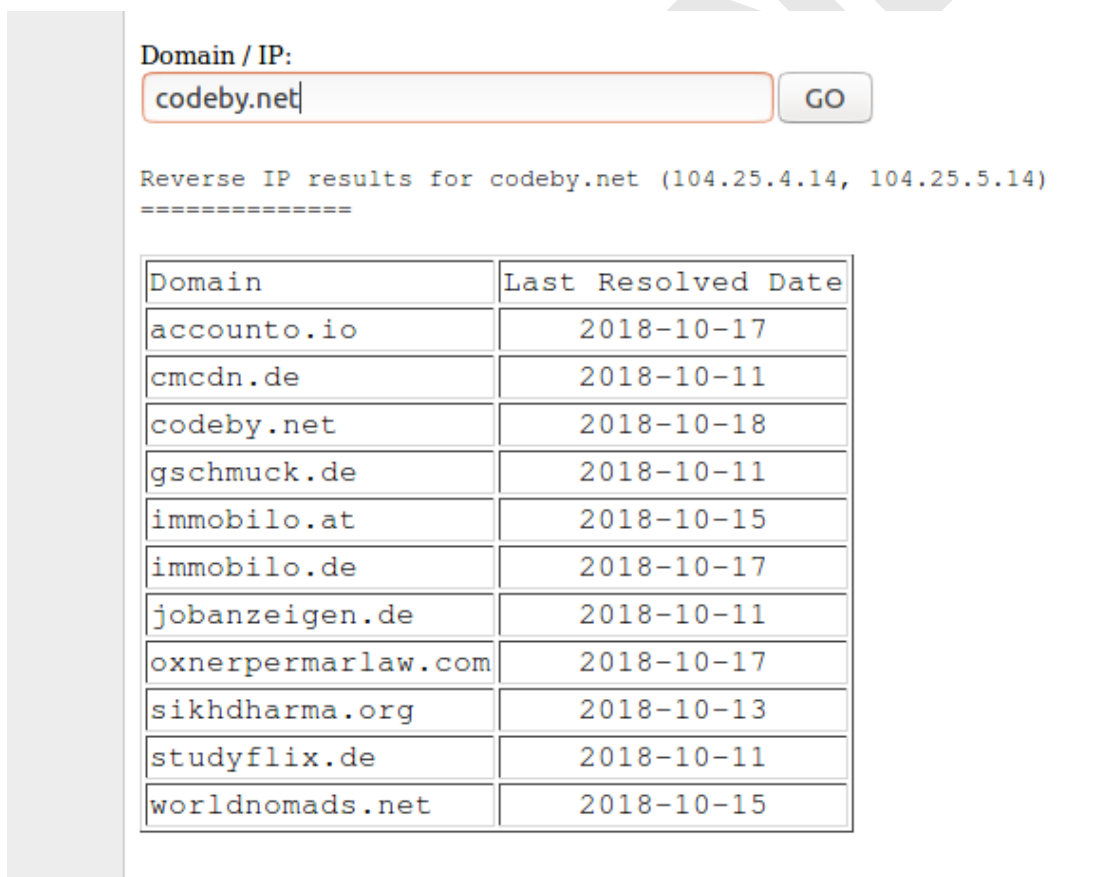
1. Присваиваем переменной NET значение подсети. Ту часть подсети, которая не меняется. Например, 192.168;
2. Обычный цикл for. \$(seq x1 x2) – вместо x1 x2 ставим цифры по которым пройдет цикл. Например, 1 127.;
3. Аналогично пункту 2;

4. Собираем IP в одной строке;
5. Используем `dig` и передаем в него полученную строку.

Далее сохраняем все это в файл с расширением `sh`. Делаем его исполняемым командой `chmod +x` и запускаем.

Если перебор необходим по 4 октету, то достаточно убрать один цикл вместе с `done`.

Также бывают случаи, когда на одном IP адресе находятся несколько сайтов. Проверить это можно с помощью следующего сервиса: viewdns.info/reverseip



Domain / IP:

Reverse IP results for codeby.net (104.25.4.14, 104.25.5.14)
=====

Domain	Last Resolved Date
accounto.io	2018-10-17
cmcdn.de	2018-10-11
codeby.net	2018-10-18
gschmuck.de	2018-10-11
immobilo.at	2018-10-15
immobilo.de	2018-10-17
jobanzeigen.de	2018-10-11
oxnerpermarlaw.com	2018-10-17
sikhdharma.org	2018-10-13
studyflix.de	2018-10-11
worldnomads.net	2018-10-15

Почтовая служба

Хотя веб сайты представляют лицо коммерческой организации, их почтовые системы обеспечивают основные деловые коммуникации.

Также почтовые системы часто слабо защищены, тем самым позволяя собрать немало информации о компании, проанализировав почтовые службы.

SMTP заголовки

Большую ценность имеют smtp заголовки, так как благодаря им можно получить такую информацию как: информация о маршрутизации, адреса и имена серверов, схемы IP, тип и версия фильтра или антивирусного решения, и даже версию почтового клиента.

```
Delivered-To: xxx@gmail.com
Received: by 2002:ac0:b65d:0:0:0:0 with SMTP id n29-v6csp2669855ime;
Sun, 1 Jul 2018 00:25:04 -0700 (PDT)
X-Google-Smtp-Source:
AAOMgpc74uhnd18ZWmp3CkhxxxJz+mDdHRhIIYffVQPlsxxxIQG2Ir+nXSHJ3Xx2Di
JGJkN2gRJ
X-Received: by 2002:a9d:6288:: with SMTP id x8-
v6mr9524320otk.159.1530429904818;
Sun, 01 Jul 2018 00:25:04 -0700 (PDT)
ARC-Seal: i=1; a=rsa-sha256; t=1530429904; cv=none;
d=google.com; s=arc-20160816;
b=jZ1wB3kna8BhRe+fc7J4AA+wHHIVKaQU2sYLg+zOXqUoieSNhVFoaJLG+UHRhS
V1Ts
ElJJv7Bo0zpdb4pIPzF8KsHZkFUqJktccAV8CHKf7EuYul44g9ILC0iyikeHH2r5uVYE
u1HWqqFtShsrxxnbjR6xvCbUxcifMLGBd3xxxIkKfMCoKFWxxxtFfB80YsbA7us3M
gw
1ziehVMxdEeHyxzPql/jMI/RhCjWBInq9T02VoEXIWsfhbt3/HrJFISw3bX6wkkUS/R
b
nNqRoFuBxDIoYtGn84Im37aHYMkL77WtWf4E5PJx1iQSVMKje053Kedr2buBXwR
yWvuq
kJyQ==
ARC-Message-Signature: i=1; a=rsa-sha256; c=relaxed/relaxed; d=google.com;
s=arc-20160816;
h=message-id:mime-version:content-disposition
:content-transfer-encoding:date:from:subject:to:dkim-signature
:arc-authentication-results;
bh=FljG23Jhe8WTYar9RxNoCv3ySWxgwq2wYUB0Jp0WSGk=;
```


b=xs34a8tm6A5+NG4t8u0E71FPg4SrwDSv4aalJP0ABPTOzD8Uaa+Oj4n/aAbPl3a
0F
2Wljs3V+wQ2BoD6IAW8EvY8ckopZUiQcVeLXGSIU+4L6aMPRHR9vcoaigZIP2rQO
eQVq
BCoZDgTph5rTjrBarTOXpiOxx2GL7oxmNahMtipVeoNxxvbGxOodsdf8WCsWRadn
n
jPwBhOtGyBzXfxVjT5+D5gxE9f4RpwVX9iX3pct3nzTjv8SyNnPvD/UsvNugAcSd4X0
Q
CFQX6gn8hHx7DFDdpq/nCWskBcxrCQfVoeuMipShsAvDq0Xyn0b5XaB1/aeSyhuC
To0x
aOGA==
ARC-Authentication-Results: i=1; mx.google.com;
dkim=pass header.i=@grindinggear.com header.s=xxfexxle
header.b=Gu51hoYf;
spf=pass (google.com: domain of support@grindinggear.com designates
192.xxx.xxx.194 as permitted sender)
smtp.mailfrom=support@grindinggear.com;
dmarc=pass (p=QUARANTINE sp=QUARANTINE dis=NONE)
header.from=grindinggear.com
Return-Path: <support@grindinggear.com>
Received: from mail3.xxx.com (mail3.xxx.com. [192.xxx.xxx.194])
by mx.google.com with ESMTPS id r9-
v6si4098545oih.358.2018.07.01.00.25.04
for <xxx@gmail.com>
(version=TLS1_2 cipher=ECDHE-RSA-AES128-GCM-SHA256 bits=128/128);
Sun, 01 Jul 2018 00:25:04 -0700 (PDT)
Received-SPF: pass (google.com: domain of support@grindinggear.com
designates
192.xxx.xxx.194 as permitted sender) client-ip=192.xxx.xxx.194;
Authentication-Results: mx.google.com;
dkim=pass header.i=@grindinggear.com header.s=paxxxfexxxe
header.b=Gu51hoYf;
spf=pass (google.com: domain of support@grindinggear.com designates
192.xxx.xxx.194 as permitted sender)
smtp.mailfrom=support@grindinggear.com;
dmarc=pass (p=QUARANTINE sp=QUARANTINE dis=NONE)
header.from=grindinggear.com
Received: from uspg2a.xxx.com (uspg2a [10.xxx.xxx.33]) by
mail3.patxxxixxe.com

(Postfix) with ESMTP id 6534F1B00294 for <xxx@gmail.com>; Sun,
1 Jul 2018 19:25:04 +1200 (NZST)
DKIM-Signature: v=1; a=rsa-sha256; c=simple/simple; d=grindinggear.com;
s=patxxxexixxle; t=1530429904;
bh=FljG23Jhe8WTYar9RxxxxxySWxgwq2wYUB0Jp0WSGk=;
h=To:Subject:From:Date;
b=Gu51hoYf1QEgnxTlc7O3qx+HxxxW/OJUF4il/l7Z/y66W9QFN3MNcD8Bqytq94
wS
4GZrQ3a3tmas3yb+j5LdRfnnjOeCthPCxxxlejl1NmVHrrjxTsAtOvnMxUdOf+rBB
JbrHUNP43Bwr9x526olkTCvMFDIWIVIsuFMbHJhQ=
Received: from localhost (localhost [127.0.0.1]) by uspg2a.xxx.com (Postfix)
with ESMTP id 5B3A9E803BF for <xxx@gmail.com>; Sun,
1 Jul 2018 19:25:04 +1200 (NZST)
To: xxxixxx <xxx@gmail.com>
Subject: Password reset
From: xxx of xxx <support@grindinggear.com>
Date: Sun, 01 Jul 2018 07:25:04 +0000
Content-Type: text/plain; charset=UTF-8
Content-Transfer-Encoding: quoted-printable
Content-Disposition: inline
MIME-Version: 1.0
Message-Id: <20180701072504.5B3A9E803BF@uspg2a.xxx.com>
Your request to reset your password has been received
Account name: xxx
Please visit the following URL to reset your password
[https://xxx.com/account/reset-password/xxx/KZBwxxxVENKQ4i-PrQc=
_lurFysCzG3a3dYBGbk5j](https://xxx.com/account/reset-password/xxx/KZBwxxxVENKQ4i-PrQc=_lurFysCzG3a3dYBGbk5j)

Это приблизительный пример. По флагам Received можно отследить, как передвигался пакет от источника к получателю. Указываются IP адреса, а также их доменные имена.

Важную информацию несет и сам Email адрес. Во многих компаниях для каждого сотрудника заводится почтовый ящик, и его имя формируется из имени сотрудника. Это имя может использоваться для входа в систему, поэтому важно собирать и всевозможные email адреса компании и сотрудников.

Анализ фактических имен, используемых для определения каждого сетевого узла или службы

Название раздела говорит о том, что наименование узлов и служб, как и принцип формирования этого имени, может дать много полезной информации. Например:

- msc.office02.example.com – может сказать о расположении офиса в Москве;
- mailSbp.example.com – почтовый сервер базирующийся в Питере;
- uxsrv.example.com – хост использует Unix систему.
- andreevPC.example.com – хост сотрудника компании с фамилией Андреев.

Также к этому разделу я отнесу и сбор информации с помощью *traceroute*, так как результат выполнения этой команды тоже имена хостов.

```
traceroute to xxx.net (xxx.xxx.xxx.xxx), 30 hops max, 60 byte packets
1 192.168.10.50 (192.168.10.50) 5.332 ms 5.473 ms 5.710 ms
2 * * *
3 37.xxx.xxx.157 (37.xxx.xxx.157) 10.689 ms 10.855 ms 11.019 ms
4 mskn08.transtelecom.net (188.xxx.xxx.6) 11.181 ms 11.389 ms 11.561 ms
5 transtelecom-ic-313016-ffm-b1.c.telia.net (213.xxx.xxx.66) 47.604 ms 50.196 ms 68.589 ms
6 ffm-b1-link.telia.net (213.xxx.xxx.65) 54.851 ms 45.122 ms 45.805 ms
7 ffm-bb4-link.telia.net (62.xxx.xxx.6) 58.573 ms ffm-bb4-link.telia.net (62.xxx.xxx.161) 63.507 ms
8 ffm-bb4-link.telia.net (62.xxx.xxx.163) 69.568 ms
9 prag-bb1-link.telia.net (62.xxx.xxx.119) 55.162 ms 56.332 ms 54.944 ms
10 prag-b3-link.telia.net (62.xxx.xxx.219) 52.904 ms 58.596 ms 69.610 ms
11 213.xxx.xxx.91 (213.xxx.xxx.91) 64.912 ms 53.883 ms 53.879 ms
11 mlc.xxx.cas.ip-xxx.net (81.xxx.xxx.22) 54.885 ms 54.824 ms 54.270 ms
12 xxx.cas.ip-xxx.net (xxx.xxx.xxx.xxx) 60.060 ms 54.774 ms 54.176 ms
```

Благодаря трассировке можно узнать, где хостится сайт, а также, где находятся дата центры.

Можно воспользоваться сторонними сервисами:

- 2whois.ru
- centralops.net

Фактический анализ сайта

Само собой, фактический анализ сайта - это обязательная составляющая пассивного сбора информации. Если сайт достаточно большой, то лучше всего проводить анализ, предварительно скачав его себе.

При фактическом анализе сайта собирается такая информация как:

1. адреса электронной почты;
2. анализ ответов сотрудников компании, которые имеют доступ к управлению сайтом;
3. анализ инструментов, используемых сотрудниками компании, информация о которых может находиться в метатегах или других скрытых полях;
4. анализ URL-ссылки на файлы;
5. анализ методов подключения;
6. анализ того, как кодирует информацию сайт;
7. анализ реакции сайта на запрос о несуществующем ресурсе;
8. анализ ссылок, ведущих на внешние ресурсы;
9. анализ заголовков http запросов к сайту, аналогично тому, как это делаете в части про email.

К этому пункту можно отнести и сбор информации о сотрудниках.

Социальная инженерия является самым эффективным способом взлома, а учитывая то, что информационные технологии плотно сплелись с повседневной жизнью почти каждого человека, собирать информацию о сотрудниках необходимо. Узнавать контактные данные, прописки, возраст, увлечения и так далее.

Воспользуйтесь следующими сервисами:

- yasni.com – агрегирует информацию по заданному имени из всей сети.

robots.txt

robots.txt – это обычный текстовый файл, в котором указаны инструкции поисковым роботам, какие директории сайта можно индексировать, а какие нет. Само собой, раз владелец указывает там директории, которые он не хочет показывать, значит нам надо их посмотреть более внимательно.

Подобную пользу могут принести sitemap.xml, а также мета теги robots.

Поисковые системы

Этот раздел является наиболее важным, так как умение пользоваться поисковыми системами - это залог успеха в нашем деле. Поисковые системы настолько важны, что по сути, могут заменить все предыдущие методы.

Благодаря поисковым системам можно собрать большое количество информации, такой как:

- имена сотрудников;
- имена директоров;
- географическое расположение;
- чем занимается организация;
- история организации и ее сотрудников;
- увлечения сотрудников;
- увлечения директоров;
- почтовые данные;
- распорядок дня компании;
- имена партнеров, которые сотрудничают с целевой компанией;
- дыры на сайте компании;
- кто админ сайта, его личную информацию, увлечения, спал ли он сегодня, что он ел, с кем дружит и многое-многое другое.

Для поиска такой информации используются так называемые “дорки”. “Дорки” - это набор запросов, использующих специальные аргументы строки запросов, которые позволяют сузить круг поиска для конкретной цели.

Все примеры ниже будут показаны на основе поисковой системы google.

Основные операторы строки запроса:

1. `site` – поиск по конкретному сайту;
2. `inurl` – поиск по вхождению в строку url;
3. `intitle` – поиск по вхождению в строку тега title;
4. `intext` – поиск по содержимому сайта;
5. `filetype` – поиск файлов конкретного типа;
6. `|` - оператор OR. Логическое ИЛИ;
7. `""` - кавычки указывают на поиск точного соответствия;
8. `-` - использует как исключение из выдачи результата;
9. `*` - означает строку любого содержания и длины.

Примеры того, как этим пользоваться:

- `"слово" site:example.com` – поиск внутри сайта по конкретному слову
- `@example.com site:example.com` – найдет почтовые адреса сайта example.com
- `"название файла" filetype:doc site:example.com` – найдет файлы с расширением doc на сайте example.com
- `inurl:example.com/*.php?id=` - найдет все php документы на сайте example.com, в url адресе которого будет ключ id.
- `Site:*.example.com` – найдет некоторые поддомены сайта example.com

Shodan

Shodan – это поисковая система, которая позволяет пользователю находить определенные хосты (веб-камеры, серверы, маршрутизаторы и так далее), подключенные к сети интернет.

Сервисом можно воспользоваться по адресу: www.shodan.io

По сути shodan - это поисковик, поэтому использовать его мы будем примерно так же, как и другие поисковики (например, google).

Для начала проверим, что нам даст простой поиск по доменному имени:



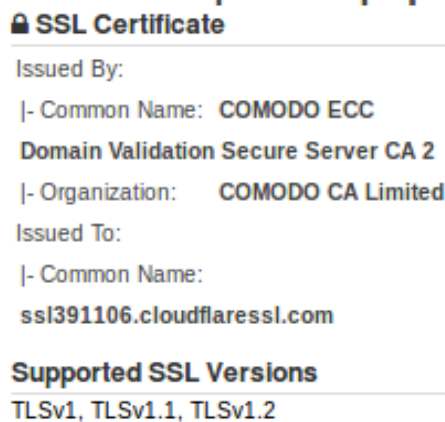
В итоге получаем следующее:

104.25.4.14
Cloudflare
Added on 2018-10-13 19:36:40 GMT

Один из IP адресов и имя обслуживающей компании:



Местоположение и используемые сервисы на сайте:



Информация об SSL сертификатах.


Теперь нажмем на ссылку “Details” или просто произведем запрос по IP адресу. В итоге получаем:

Country	United States
Organization	Cloudflare
ISP	Cloudflare
Last Update	2018-10-23T03:09:57.570918
ASN	AS13335


Эту информацию мы уже давно знаем.


Информация о сервисах, используемых на сайте:


⚡ Web Technologies


 All In One SEO Pack


 Bootstrap

 Google Analytics


 Google Font API

 JQuery

 JQuery Migrate

 MySQL

 PHP

 WordPress

 Zepto

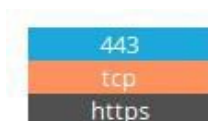
Открытые порты:

Ports



В разделе Services представлена информация о том, что ответил сервис на запрос по порту от shodan.

Например:



```
HTTP/1.1 200 OK
Date: Sat, 13 Oct 2018 19:36:40 GMT
Content-Type: text/html; charset=UTF-8
Transfer-Encoding: chunked
Connection: keep-alive
Set-Cookie: __cfduid=d32fc6e8adfe5a41c1b3cffe99a3821371539459399; expires=Sun, 13-Oct-19 19:36:39 GMT; path=/; domain=.codeby.net; HttpOnly; Secure
Link: <https://codeby.net/wp-json/>; rel="https://api.w.org/", <https://codeby.net/>; rel=shortlink
Strict-Transport-Security: max-age=0; includeSubDomains; preload
X-Content-Type-Options: nosniff
Expect-CT: max-age=604800, report-uri="https://report-uri.cloudflare.com/cdn-cgi/beacon/expect-ct"
Server: cloudflare
CF-RAY: 4694419f2b611401-LAX
```

Как и в поисковике google, в shodan тоже есть операторы поиска:

net – поиск по IP:



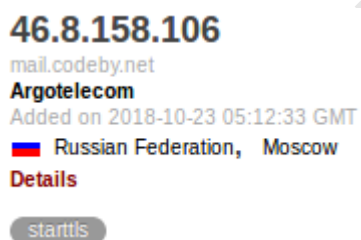
В итоге получили названия сервисов на сайте:

HTTPS (8443)	1
HTTP (8080)	1
WHM + SSL	1
WHM	1
cPanel + SSL	1

Hostname – поиск по доменному имени:



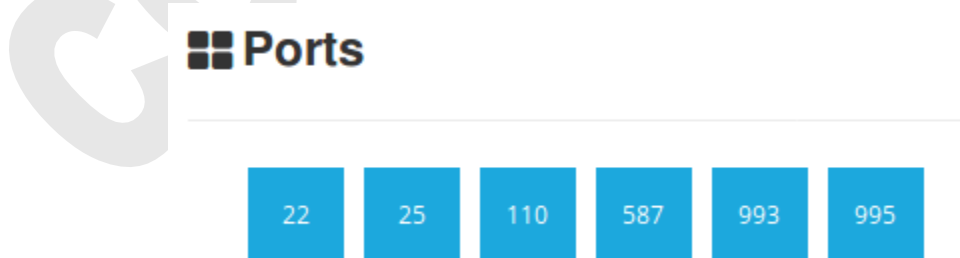
В итоге найден почтовый шлюз:



Найдены новые сервисы:

POP3 + SSL	1
IMAP + SSL	1
587	1
POP3	1
SMTP	1

Новые открытые порты:



Другие операторы:

City – поиск по определенному городу

City: "London"

Country – поиск по определенной стране

country: "Japan"

Geo – поиск по координатам

geo: 45.4545,-45.4545

Os – поиск по определенной операционной системе

os: "windows server 2008"

Port – поиск по определенному порту

port: 21

Есть еще аналоги, например, Censys (censys.io) или Zoomeye (zoomeye.org). Все они работают по разным алгоритмам, поэтому стоит проверять на нескольких сразу.

Vulners

Vulners (vulners.com) – это база данных, в которой хранится такая информация как патчи, эксплойты, уязвимости, результаты bug bounty.

Другими словами, благодаря vulners можно получить такую информацию как:

- отчеты по багам продуктов вендоров, которые они сами и выкладывают;
- эксплойты из exploit-DB и Metasploit;
- общее описание уязвимостей и ссылки на источники;
- публикации на тематических ресурсах;
- nessus-плагины для определения уязвимостей.

Vulners позволяет производить не только простые запросы типа "wordpress" или "example.org", но и использовать операторы для фильтрации результата.

- Type:amazon – поиск по определенному вендору;
- csvv.score:[1 TO 5] – поиск по уровню критичности от 1 до 5;
- order:Published - сортировка по дате публикации;
- last 10 days – за последние 10 дней

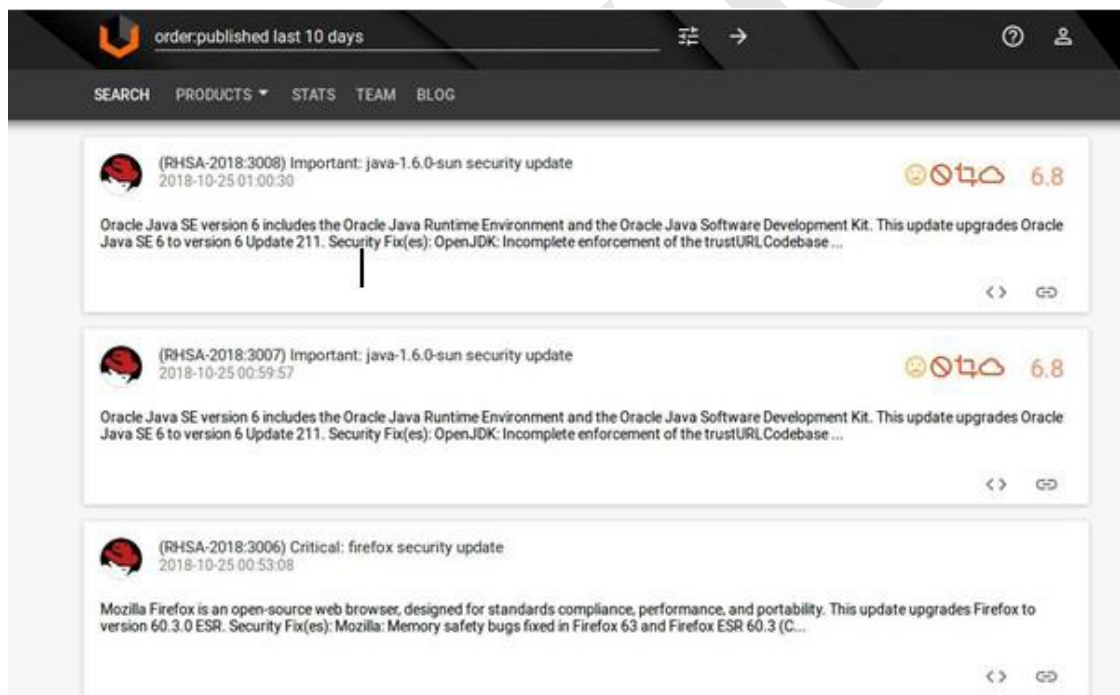
Сам поисковик выглядит так:



А так выглядит запрос:

order:published last 10 days

Запрос должен показать публикации за последние 10 дней. В результате:



Анализ SSL сертификатов

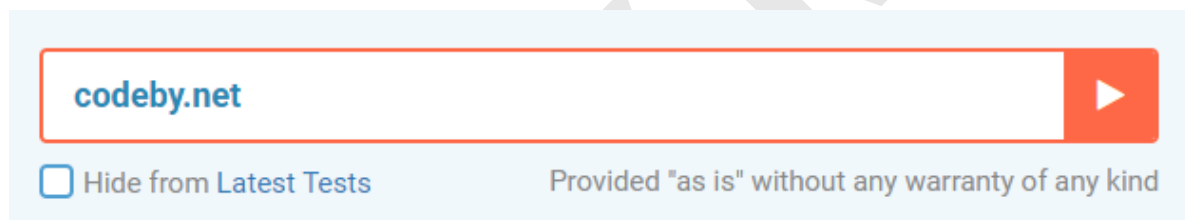
SSL/TLS протокол в наше время является обязательным для интернет коммуникаций. Он используется для таких вещей как: передача платежных реквизитов, администрирование виртуальной облачной

инфраструктуры, сохранение переписки в мессенджерах, аутентификация серверов в мобильных приложениях, пересылка локальных данных в облачное хранилище.

Уязвимости данного протокола дают доступ к широкому спектру MitM атак (Man In the Middle – человек посередине). Чтобы обнаружить эти уязвимости, необходимо анализировать SSL сертификаты. Для подобной задачи существует большое количество сервисов, но я хочу рассказать вам про два, которые, помимо информации о самих сертификатах, дают дополнительную информацию о целевом сайте.

Free SSL Server Test immunivweb.com/ssl

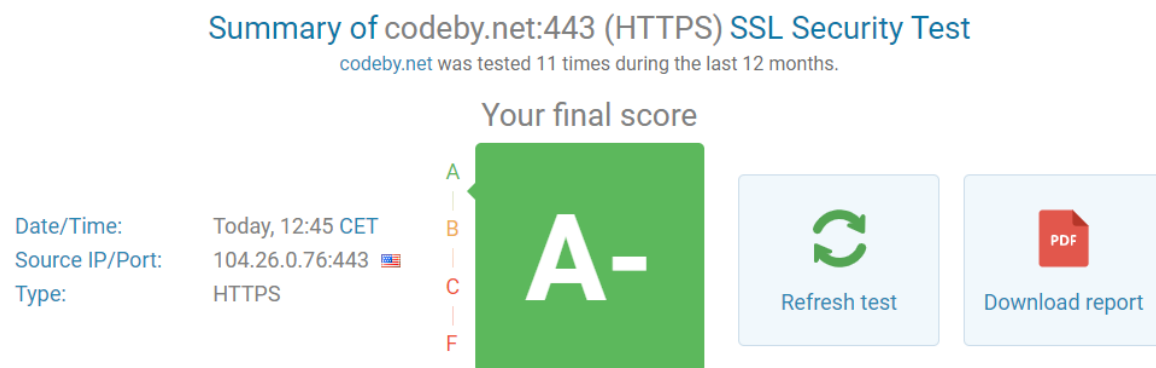
Встречает нас следующий интерфейс.




The screenshot shows the interface of the 'Free SSL Server Test' service. At the top, there is a search bar containing the text 'codeby.net' and a red play button. Below the search bar, there is a checkbox labeled 'Hide from Latest Tests' and a disclaimer: 'Provided "as is" without any warranty of any kind'.

Обычное поле для запроса, ничего необычного. Попробуем проверить codeby.net

В итоге видим следующее:





The screenshot displays the results of an SSL Security Test for 'codeby.net:443 (HTTPS)'. The title is 'Summary of codeby.net:443 (HTTPS) SSL Security Test'. Below the title, it states 'codeby.net was tested 11 times during the last 12 months.' The main result is 'Your final score' which is 'A-'. To the left of the score, there is a vertical scale from A to F. To the right of the score, there are two buttons: 'Refresh test' and 'Download report'. On the far left, there is a table with test details:

Date/Time:	Today, 12:45 CET
Source IP/Port:	104.26.0.76:443 
Type:	HTTPS

Общая оценка сертификата “A”, что говорит о том, что с безопасностью сертификата должно быть все хорошо.

Заодно сервис проводит проверку поддоменов.

Discovered Email Servers and Subdomains					
Hostname	Protocol/Port	Certificate(s)	Tested on	Compliant with	Grade
school.codeby.net	HTTPS / 443	 	December 4th 2020, 15:09		A
www.pentest.codeby.net	SMTP / 25	?	December 5th 2019, 16:36		F
www.pentest.codeby.net	POP3 / 110	?	December 4th 2019, 17:37		F
www.pentest.codeby.net	IMAP / 143	?	November 26th 2019, 07:33		F
SHOW 37 MORE					
Discover all your subdomains, APIs and public cloud storage with ImmuniWeb Discovery .					
FREE DEMO					

Ниже на странице можно наблюдать подробную информацию о выданных сертификатах:

SSL Certificate Analysis	
RSA CERTIFICATE INFORMATION	
Issuer	Cloudflare Inc RSA CA-2
Trusted	Yes
Common Name	sni.cloudflaressl.com
Key Type/Size	RSA 2048 bits
Signature Algorithm	sha256WithRSAEncryption
Subject Alternative Names	DNS:*.codeby.net, DNS:codeby.net, DNS:sni.cloudflaressl.com
Transparency	Yes
Validation Level	OV
CRL	http://crl3.digicert.com/CloudflareIncRSACA-2.crl
OCSP	http://ocsp.digicert.com
OCSP Must-Staple	No
Supports OCSP Stapling	Yes
Valid From	June 11th 2021, 01:00 CET
Valid To	June 11th 2022, 00:59 CET

Еще ниже расположены результаты проверки на популярные уязвимости:

POODLE OVER TLS ⓘ	
The server is not vulnerable to POODLE over TLS.	Not vulnerable
GOLDENDOODLE ⓘ	
The server is not vulnerable to GOLDENDOODLE.	Not vulnerable
Zombie POODLE ⓘ	
The server is not vulnerable to Zombie POODLE.	Not vulnerable
Sleeping POODLE ⓘ	
The server is not vulnerable to Sleeping POODLE.	Not vulnerable
0-Length OpenSSL ⓘ	
The server is not vulnerable 0-Length OpenSSL.	Not vulnerable
CVE-2016-2107 ⓘ	
The server is not vulnerable to OpenSSL padding-oracle flaw (CVE-2016-2107).	Not vulnerable
SERVER DOES NOT SUPPORT CLIENT-INITIATED INSECURE RENEGOTIATION ⓘ	
The server does not support client-initiated insecure renegotiation.	Good configuration

На этом наш урок подошел к концу. Пришло время проверить ваши навыки на практике. Вам уже доступен документ, расположенный в разделе "Методические материалы" под названием "Инструкция для начала практических занятий". Задания по данной теме расположены в одноименном разделе площадки. Каждое задание создано для отработки основных навыков пассивного сбора информации. Информации в уроке достаточно, чтобы решить любое из них.



Служба Поддержки

8 800 707 5466

с 8:00 до 20:00 МСК

school@codeby.net